Abstract Algebra 3H and Beyond

L. Foskett M. Kiwan E. Ferguson

Jan 2024

Contents

§1 Lecture 1

Definition 1.1. A *group* is a pair $(G, *)$, where G is a set and $* : G \times G \to G$ is a binary operation, that satisfies the following axioms:

(G1) Associativity: for any $g, h, k \in G$,

$$(g * h) * k = g * (h * k);$$

(G2) Existence of identity: there exists $e \in G$ such that for any $g \in G$,

$$e * g = g * e = g;$$

(G3) Existence of inverses: for any $g \in G$ there exists $h \in G$ s.t.

$$g * h = h * g = e.$$

We should note that we are assuming G is closed under the binary operation, but in general we should verify that the product of two elements of G stays in G. Often we will omit the binary operation so that $g * h$ is shortened to just gh.

Also, from the second axiom we can immediately deduce that the identity in a group must be unique. We will typically use e or 1 to denote the identity element of a group, but when there is the possibility of ambiguity we will use 1_G to denote the identity element in the group G.

Theorem 1.2

Let G be a group and $g \in G$ with left inverse h and right inverse h', i.e.

$$h * g = g * h' = e \in G.$$

Then $h = h'$.

Proof. We have that

$$h = h * e = h * (g * h') = (h * g) * h' = e * h' = h',$$

by direct application of the group axioms. □

Note that the above also implies that the inverse is unique, and we need not make the distinction between left and right inverses in a group. We denote the inverse of an element $g \in G$ as g^{-1}.

Proposition 1.3

Let G be a group and $g, h \in G$. Then we have

1. $(g^{-1})^{-1} = g$,
2. $(gh)^{-1} = h^{-1}g^{-1}$.

Proof. (1) The inverse of g^{-1} is an element $x \in G$ that satisfies $xg^{-1} = g^{-1}x = e$.

Taking the second equality, we can left multiply by g to get

$$gg^{-1}x = g \implies x = g.$$

(2) We can verify that

$$\begin{aligned}(gh)(h^{-1}g^{-1}) &= g(hh^{-1})g^{-1} \\ &= geg^{-1} \\ &= gg^{-1} \\ &= e,\end{aligned}$$

meaning that the element $h^{-1}g^{-1}$ is the unique inverse of gh. □

Proposition 1.4

Let G be a group and $g, h, k \in G$. Then the following are equivalent:

1. $gh = gk$,
2. $h = k$,
3. $hg = kg$.

Proof. If $gh = gk$, left multiplying by g^{-1} and applying the inverse axiom we see that $h = k$. Similarly, given that $h = k$, we can left multiply by g so that $gh = gk$.

Applying a similar argument for right multiplication shows that all three statements are equivalent. □

Definition 1.5. A group G is *abelian* if the group operation is commutative, i.e. $\forall g, h \in G$ we have $gh = hg$.

When a group is abelian, we often use additive notation to denote the group operation, as opposed to the typical multiplicative notation (e.g. powers).

Definition 1.6. We say a group is *finite* or *countable* if the underlying set is finite or countable, respectively.

§1.1 Symmetric groups

One recurring class of groups we will consider are symmetric groups.

Definition 1.7. Let X be a set. The *symmetric group* of X, denoted $\mathrm{Sym}(X)$ is the set of all permutations of the elements of X. Symbolically,

$$\mathrm{Sym}(X) = \{\sigma : X \to X \mid \sigma \text{ is a bijection}\}.$$

If $X = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, we say $\mathrm{Sym}(X)$ is the symmetric group on n letters, denoted S_n.

Remark 1.8. Symmetric groups are indeed groups under composition of permutations. It is straightforward to check that the composition of permutations is indeed a permutation, and that the remaining group axioms hold. We will later see that all finite groups can be understood within the context of a symmetric group.

Any permutation can be decomposed into a product of disjoint cycles. For example, the bijection

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

is equivalent to the composition of cycles $(123)(45)$. The notation (123) is shorthand for the permutation sending 1 to 2, 2 to 3, and 3 to 1.

§2 Lecture 2

§2.1 Subgroups and their properties

Definition 2.1. Let G be a group. A subset $H \subseteq G$ is called a *subgroup* of G if we have the following:

1. The identity element e is contained in H.
2. If $a, b \in H$, then $ab \in H$.
3. If $a \in H$, then $a^{-1} \in H$.

In other words, H is a subset of G that is a group in its own right, with the same identity and same group operation. We write $H \leq G$ to denote a subgroup.

Proposition 2.2 (Subgroup test)
Let H be a subset of a group G. Then H is a subgroup if and only if the following hold:

1. H is non-empty.
2. If $x, y \in H$ then $x^{-1}y \in H$.

Proof. ($\implies$) The first holds since $e \in H$. Let $x, y \in H$. Since H is a group, it is closed under taking inverses, so $x^{-1} \in H$. Also, H is closed under the group operation of G, so $x^{-1}y \in H$, as desired.

($\impliedby$) We have that H is non-empty and that for any $x, y \in H$ we have $x^{-1}y \in H$. We claim that H contains the identity, is closed, associative, and every element has an inverse in H.

Since H is non-empty, let $x \in H$. By the second property with $y = x$ we have $x^{-1}x = e \in H$. If $x \in H$, we have $x^{-1}e = x^{-1} \in H$, so H is closed under taking inverses. Now for two elements $x, y \in H$, we have shown that $x^{-1} \in H$, so $(x^{-1})^{-1}y = xy \in H$, and hence H is closed under the binary operation. Finally, associativity holds since the binary operation in G is associative. □

Definition 2.3. A group G is called *cyclic* if there exists a $g \in G$ such that

$$G = \{g^n \mid n \in \mathbb{Z}\}.$$

If G is cyclic, then such an element g is called a generator of G. We say G is generated by g, and write $G = \langle g \rangle$.

Remark 2.4. If g is a generator for G, then so is g^{-1}, since if $x \in G$ can be expressed as g^k, then $x = (g^{-1})^{-k}$.

Theorem 2.5
Every cyclic group is abelian.

Proof. Let $G = \langle g \rangle$ be a cyclic group, and let $x, y \in G$. Then $x = g^n$ and $y = g^m$ for some $n, m \in \mathbb{N}$. Now,

$$xy = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = yx.$$

Therefore G is abelian. □

Theorem 2.6
All subgroups of a cyclic group are cyclic.

Proof. Let $H \leq G$ where G is a cyclic group with generator g. We aim to show $\exists h \in H$ s.t. $H = \langle h \rangle = \{h^n \mid n \in \mathbb{Z}\}$. When $H = \{e\}$, the proof is trivial.

If $\exists\, n \in \mathbb{Z}_{>0}$ s.t. $g^n \in H$, assume such n is the lowest possible, without loss of generality. We claim that $H = \langle g^n \rangle$.

Assume $g^a \in H$ for some $a = qn + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $g^a = (g^n)^q g^r$, and we know $g^n q \in H$ since H is a group on its own. This means we must have $g^r \in H$, but n was the smallest possible power of g, so $r = 0$, i.e. $g^r = e$, and hence $g^a = g^{nq} = (g^n)^q$, i.e. H is cyclic with generator g^n. □

Definition 2.7. The *order* of a group G, written $|G|$, is the cardinality of the underlying set. If G is an infinite group, we say $|G| = \infty$.

If $g \in G$, we say the order of g, written $|g|$ or $\text{ord}(g)$, is the smallest positive integer n such that $g^n = e$. We say $|g| = \infty$ if no such n exists.

Theorem 2.8
Let G be a group, and let $g \in G$. Then the order of g is equal to the order of the subgroup $\langle g \rangle \leq G$.

Proof. If $|g| = m < \infty$, then $\langle g \rangle = \{1, g, g^2, \cdots, g^{m-1}\}$, so $|g| = m$.

If the order of g is infinite, then $\langle g \rangle = \{e, g, g^2, g^3, \ldots\}$ with no repeats, since if $i < k$ with $g^i = g^k$, then $g^{k-i} = e \implies k - i = 0$. Therefore $|\langle g \rangle| = \infty$. □

Theorem 2.9

Let G be a group, and let $g \in G$, and $n \in \mathbb{Z}$. Then $g^n = e$ if and only if n is a multiple of $|g|$.

Proof. ($\implies$) Suppose $g^n = e$. There exists integers k, r with $0 \leq r < m$ such that $n = km + r$. We have $g^n = g^{km+r} = g^{km}g^r = e$. We know $g^{km} = e$, so we must have $g^n = g^r = e$. However, since $r < m$, $r = 0$. Therefore, $n = km$, as required.

($\impliedby$) Let $|g| = m$. Suppose n is a multiple of m, then $\exists$k$\in \mathbb{Z}$ s.t. $n = km$. We have,

$$g^n = g^{mk} = (g^m)^k = e^k = e,$$

as required. □

§3 Lecture 3

Theorem 3.1

Let $g \in G$ have order $n < \infty$, and fix some $k \in \mathbb{Z}$. Then $|g^k| = \frac{n}{d}$ where $d = \gcd(n, |k|)$.

Proof. The order of g^k is the smallest positive integer i such that $(g^k)^i = g^{ki} = e$. As the order of g is n, we seek the smallest i such that ki is a multiple of n. The smallest such multiple will be when $i|k| = \text{lcm}(n, |k|) = \frac{n|k|}{\gcd(n,|k|)}$. This gives $i = \frac{n}{d}$ as required.

□

Corollary 3.2

Let $G = \langle g \rangle$ be a cyclic group generated by g, and have order $n < \infty$. Fix $k \in \mathbb{Z}$. Then

$$G = \langle g^k \rangle \iff \gcd(n, k) = 1.$$

Proof. We have that g^k is a generator for $G \iff \langle g^k \rangle = \langle g \rangle \iff |g^k| = n \iff \gcd(k, n) = 1$. □

§3.1 Multiplication tables

One often helpful way to understand a small group is to construct its multiplication table.

Definition 3.3. If a group G has order n and elements $g_1, g_2, \ldots, g_n$, then a *multiplication table* for G is an $n \times n$ grid where the entry (i, j) in the i^{th} row and j^{th} column is the product $g_i g_j$ in the group.

Example 3.4

Consider the cyclic group of order 3, $C_3 = \{e, g, g^2\}$. A multiplication table for C_3 is:

	e	g	g^2
e	e	g	g^2
g	g	g^2	e
g^2	g^2	e	g

Note that we could switch g and g^2 to get the equivalent table:

	e	g^2	g
e	e	g^2	g
g^2	g^2	g	e
g	g	e	g^2

Theorem 3.5

Let G be a finite group. Then every row and column of a multiplication table for G contains each element of G exactly once.

Proof. This follows directly from the group axioms. If the (i, j) and (i, k) entries are the same, i.e. $g_i g_j = g_i g_k$, left multiplication by g_i^{-1} gives that $g_j = g_k$, so $j = k$. □

We wish to classify all possible groups of order 4 using this method. In other words, we want to find all essentially different multiplication tables for a group with 4 elements.

Let $G = \{g_1, g_2, g_3, g_4\}$ and choose g_1 to be the identity element in G. The identity axiom forces 7 entries in the multiplication table:

	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2			
g_3	g_3			
g_4	g_4			

Now we have a choice. We can either pick $g_2 g_2 = g_1$, or $g_2 g_2 = g_3$ (g_4 leads to the same structure as g_3).

Let us choose the first case, i.e. g_2 is self-inverse. If we add this to the multiplication table, the presence of $g_1, g_2,$ and g_3 in the row and column containing $g_2 g_3$ forces this to take the value g_4 (we can treat this much like a sudoku puzzle).

Once we have this breakthrough, we are able to fill in all but the lower right-hand quadrant. Again, we have a choice, so let $g_3 g_3 = g_1$ (we will come back to the other possibility later). This completes the multiplication table:

	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2	g_1	g_4	g_3
g_3	g_3	g_4	g_1	g_2
g_4	g_4	g_3	g_2	g_1

Now, we can go back to the beginning and check the case where $g_2g_2 = g_3$. By the "sudoku" property, we must have $g_4g_2 = g_1$. This alone forces the rest of the multiplication table:

	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2	g_3	g_4	g_1
g_3	g_3	g_4	g_1	g_2
g_4	g_4	g_1	g_2	g_3

The claim now is that these two group tables are the only essentially different ones. To convince ourselves of this, we can return to the previously mentioned possibility in our first complete table, and instead let $g_3g_3 = g_2$. Compare the following multiplication tables:

	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2	g_1	g_4	g_3
g_3	g_3	g_4	g_2	g_1
g_4	g_4	g_3	g_1	g_2

	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2	g_3	g_4	g_1
g_3	g_3	g_4	g_1	g_2
g_4	g_4	g_1	g_2	g_3

Notice that the permutation of rows $2 \mapsto 4 \mapsto 3 \mapsto 2$ on the left table gives us the right table, up to relabelling the elements.

In a similar way, any other possible table we could make can be permuted and relabelled to arrive at one of the two distinct multiplication tables we already have. This tells us that we only have two groups of order 4, which we call C_4 and V_4. From the multiplication tables, we can see that both groups are abelian.

> **Remark 3.6.** In general, we say two groups of the same order are "the same" if their multiplication tables are the same. We will make this notion precise later with the concept of an isomorphism.

§4 Lecture 4

§4.1 Cosets

Definition 4.1. Let G be a group and H a subgroup of G. Let $g \in G$. The *left coset* of H containing g is the set $gH = \{gh \mid h \in H\}$. Similarly, the *right coset* of H containing g is the set $Hg = \{hg \mid h \in H\}$.

Example 4.2

Let G be the symmetric group S_4 and let $H = \langle (1,2,3) \rangle = \{e, (1,2,3), (1,3,2)\}$ and let $g = (1,4)$. Then we have

$$gH = \{(1,4), (1,2,3,4), (1,3,2,4)\} \subset G.$$

Note that this is not a group itself since it doesn't have the identity; it is simply a subset of G. Moreover, the right coset

$$Hg = \{(1,4), (1,4,2,3), (1,4,3,2)\}$$

is a different coset that only has in common g. So $gH \neq Hg$.

Theorem 4.3

Let G be a group, $H \leq G$, and $g, g' \in G$. Then one has $gH = g'H \iff g'^{-1}g \in H$.

Proof. ($\implies$) Suppose $gH = g'H$. Then there exists $h \in H$ s.t. $g = g'h$, and so $g'^{-1}g = h \implies g'^{-1}g \in H$, as required.

($\impliedby$) Let $gh \in gH$. We have that $g'^{-1}g = h'$, for some $h' \in H$, so $g = g'h'$, meaning $gh = g'h'h \in g'H$, so $gH \subseteq g'H$. We can use a symmetric argument to conclude that $g'H \subseteq gH$, so $gH = g'H$. □

Example 4.4

Let $G = (\mathbb{R}, +)$ and $H = \mathbb{Z}$. We see that for $x, y \in \mathbb{R}$, we have $x + \mathbb{Z} = y + \mathbb{Z}$ if and only if $y - x \in \mathbb{Z}$, i.e. x and y differ by an integer.

Corollary 4.5 (Absorption rule)

Let G be a group and $H \leq G$, and $g \in G$. Then $gH = H \iff g \in H$.

Corollary 4.6

The relation $\sim$ on G defined by $g \sim g'$ iff $gH = g'H$ is an equivalence relation. In particular, the equivalence classes are all the left cosets of H in G.

Proof. The relation is trivially reflexive, symmetric and transitive by properties of equality. □

Remark 4.7. Note that this gives the natural conception that cosets partition the group — in a sense it allows us to look at the group on a larger scale. However, this partition is only another set; it need not necessarily conserve group structure.

Theorem 4.8

All cosets of H have the same cardinality. That is $\forall g \in G$, $|gH| = |H|$.

Proof. Fix $g \in G$ and let $\varphi : H \longrightarrow gH$ be the mapping $h \longmapsto gh$. We claim that φ is a bijection.

This is surjective since every element of gH can be recovered as gh for some $h \in H$.

If we suppose $gh = gh'$, then clearly $h = h'$ after we left multiply by g^{-1}, so φ is injective. □

§5 Lecture 5

§5.1 Counting groups and Lagrange

Definition 5.1. Let G be a group and H a subgroup. The set of left cosets of H in G is denoted by G/H, also called the set of equivalence classes generated by the equivalence relation defined in Corollary 4.6. Similarly the set of right cosets of H in G is denoted by $H \setminus G$.

Everything we have said about left cosets applies symmetrically to right cosets, since we can define a natural injective map $Ha \mapsto a^{-1}H$. However, it is important to note that the way H partitions G into left and right cosets is different in general.

Theorem 5.2 (Lagrange's theorem)
Let G be a finite group, and let H be a subgroup of G. Then $|H|$ divides $|G|$.

Proof. We have that G is the disjoint union of its left cosets. Since $\forall g \in G, |gH| = |H|$, we can observe that $|G|$ must be a multiple of $|H|$; in other words $|H|$ divides $|G|$. □

Definition 5.3. The number of (left) cosets of H in G is called the *index* of H in G, written $[G : H]$.

The index may be infinite. For example, the subgroup $\mathbb{Z}$ in $\mathbb{R}$ has uncountably infinite index.

Corollary 5.4
Let G be a finite group and H be a subgroup. Then we have that $|G| = |H| \cdot [G : H]$.

Proof. By Theorem 4.8, we have that G is the union of its cosets, which are disjoint. In other words,

$$G = \bigcup_{g \in G} gH \implies |G| = |gH|[G : H] = |H|[G : H].$$

□

Theorem 5.5
The number of left cosets of H in G equals the number of right cosets.

Proof. Define a bijection $G/H \to H \setminus G$ where $gH \mapsto Hg^{-1}$. To show injectivity, suppose $Hg^{-1} = Hg'^{-1}$ for some $g, g' \in G$. Then $\exists h \in H$ s.t. $hg^{-1} = g'^{-1}$, so $g' = gh^{-1} \in gH \implies g'H = gH$. Surjectivity follows from the fact that every element $g \in G$ has an inverse, since the left coset $g^{-1}H$ will map to $H\left(g^{-1}\right)^{-1} = Hg$. □

Note that we may have infinite-order groups but with finite index (a finite number of cosets). For example, $\mathbb{Z}$ is infinite but the subgroup $n\mathbb{Z}$ has index n.

Corollary 5.6

Let G be a finite group, and let $g \in G$. Then the order of g divides $|G|$.

Proof. Let $H = \langle g \rangle$ so that $H \leq G$. By Lagrange we have $|G| = |H| \cdot [G : H] = |g| \cdot [G : H]$, so $|g|$ divides $|G|$ since $[G : H] \in \mathbb{N}$. □

Remark 5.7. The converse is not true in general. If k divides $n = |G|$ then that does not mean there exists a subgroup H of G with order k. Despite this, the Sylow theorems for finite groups give conditions for subgroups of a specific order to exist.

Corollary 5.8

Every group of prime order is cyclic.

Proof. Let G be a group of prime order p. Since the order of $g \in G$ must divide p, either $|g| = 1$ or $|g| = p$. The only element with order 1 in any group is the identity, so the remaining $p - 1$ elements must have order p, and therefore are generators for the group. □

Example 5.9

A particular example where Lagrange's theorem is useful is the following.

Let $n \in \mathbb{N}$. The set $\{i \in \{1, 2, \cdots, n-1\} \mid \gcd(i, n) = 1\}$ forms a group under multiplication mod n, denoted $(\mathbb{Z}/n\mathbb{Z})^\times$. Note that if n is prime, then the group has order $n - 1$.

Let us work out the order of $3 \in (\mathbb{Z}/7\mathbb{Z})^\times$. By Lagrange, we know that $|3|$ must divide $|G| = 6$, so $|3|$ can be either $2, 3$, or 6. It's not hard to see that $3^2 = 9 = 2 \mod 7$ and $3^3 = 2 \cdot 3 \mod 7 = 6 \mod 7$, so we must have $|3|$ indeed has order 6. Since the group is of order 6 and we found an element of order 6, we also discovered that the group is cyclic (3 is a generator).

§6 Lecture 6

§6.1 Normal subgroups and Quotients

Recall that G/H is a set and does not necessarily preserve the group structure of G. We want to explore when it does. When do the set of left (or right) cosets form a group

under coset multiplication, defined as

$$xH \cdot yH = xyH$$

for $x, y \in G$? The problem we run into is ensuring well-definedness, that taking different representatives of the same coset gives us the same result. So, when does $xH = x'H$ and $yH = y'H \implies xyH = x'y'H$?

First, let us look at a non-example. In S_3, consider the subgroup $H = \langle (12) \rangle = \{e, (12)\}$. We have that $(123)H = (13)H$ and $(132)H = (23)H$. Now, if we multiply these two cosets together using different representatives, we find that

$$(13)H(23)H = (13)(23)H = (132)H,$$

but

$$(123)H(132)H = (123)(132)H = H,$$

so the coset multiplication is not well-defined in this case.

We can notice that, for example,

$$(13)H = \{(13), (123)\} \neq \{(13), (132)\} = H(13).$$

It turns out that equality between left and right cosets $xH = Hx$ (normality) is exactly the condition we need to make this work, as seen later by Theorem 6.3.

Definition 6.1. Let G be a group and let $H \leq G$. The subgroup H is called *normal* in G, denoted $H \triangleleft G$, if for all $x \in G$ we have $xH = Hx$.

The maximal and trivial subgroups of any group are normal. $G \leq G$ has only one coset so the condition is automatically satisfied. Similarly, if $H \leq G$ is trivial, then

$$xH = \{xe\} = \{x\} = \{ex\} = Hx.$$

Also, any subgroup of an abelian group is normal, since

$$xH = \{xh \mid h \in H\} = \{hx \mid h \in H\} = Hx.$$

Theorem 6.2 (Equivalent conditions for normality)

Let G be a group and $H \leq G$. Then the following are equivalent:

- $\forall x \in G$, $xH = Hx$
- $\forall x \in G, \exists y \in G$ s.t. $xH = Hy$
- $G/H = H \setminus G$
- $\forall x \in G$, $xHx^{-1} = H$
- $\forall x \in G$, $xHx^{-1} \subseteq H$
- $\forall x \in G$, $\forall h \in H$, $xhx^{-1} \in H$

Proof. See 2F. □

Theorem 6.3

Let G be a group and $H \leq G$. Then multiplication of (left) cosets of H in G, defined for all $aH, bH \in G/H$ by

$$aH \cdot bH = abH$$

is well defined if and only if H is normal in G.

Proof. ($\implies$) Suppose the operation is well defined, i.e., if $xH = x'H$ and $yH = y'H$ then $xyH = x'y'H$.

We aim to show that $xH = Hx$. Let $x' \in xH$, so we have that $xH = x'H$. Then we can say

$$x^{-1}x'H = x^{-1}Hx'H = x^{-1}HxH = x^{-1}xH = eH = H.$$

Therefore, there exists $\widetilde{h}$ such that $x^{-1}x' = h$ so $x' = \widetilde{h}x \in Hx$, meaning $xH \subseteq Hx$. We also have $x' \in Hx$ implies $x' \in xH$ by a symmetric argument. Therefore $xH = Hx$.

($\impliedby$) Suppose $H \triangleleft G$, and let $xH = x'H$ and $yH = y'H$. Then we have $x' = xh$ and $y' = yh'$ for some $h, h' \in H$. Then

$$x'y'H = xhyh'H = xhyH.$$

By our normality condition, there exists $\hat{h}$ s.t. $hy = y\hat{h}$. Therefore, $x'y'H = xhyH = xy\hat{h}H = xyH$ as required. □

We can now define the quotient group of a group by its normal subgroups.

Definition 6.4. Let G be a group, and N be a normal subgroup. The set of left cosets G/N together with the binary operation $(gN)(hN) = (gh)N$ for $g, h \in G$ is called the *quotient group* or *factor group* of G by N.

Note that by the definition of normal subgroups, we have that normal subgroup's left cosets equal that subgroup's right cosets, since $gNg^{-1} = N \iff gN = Ng$.

Example 6.5

Consider the group S_3. We claim the subgroup generated by (123) is normal. Indeed, it is the group consisting of the identity and all 3-cycles in S_3. Since conjugation preserves the cycle type of a permutation, the claim follows (since any conjugation will be a 3-cycle, which is contained in the subgroup).

In contrast, the subgroup generated by (12) is not normal. For instance, we have

$$(13)(12)(13) = (23) \notin \langle (12) \rangle.$$

Theorem 6.6

Let G be a group and $H \leq G$ of index 2. Then H is normal in G.

Proof. Let H be a subgroup of G of index 2. Then $[G : H] = 2$ so there are two left cosets and two right cosets of H in G. One of the cosets is $eH = He = H$. Now, take an element of G that is not in H, $g \in G \setminus H$. Since cosets form a partition of the group, the

other coset must be the rest of the group. In other words, $gH = Hg = G \setminus H$. We have shown that left and right cosets are equal, therefore H is normal in G.

□

Example 6.7

Recall that we can write a permutation as a product of transpositions (2-cycle permutations), and the *parity* of the number of transpositions is invariant (doesn't depend how you write the product). So a permutation is even if it can be written as an even number of transpositions, and it's odd otherwise. Hence we define the sign of a permutation to be $+1$ or -1 depending on whether it's even or odd, respectively. We can note also that the sign of a permutation must be the same as its inverse, since the function

$$\begin{aligned} \operatorname{sgn} : S_n &\to \{+1, -1\} \\ \sigma &\mapsto \begin{cases} +1, & \text{if } \sigma \text{ is even} \\ -1, & \text{if } \sigma \text{ is odd} \end{cases} \end{aligned}$$

is a homomorphism.

Let $n \in \mathbb{N}$ and let $A_n \subset S_n$ be the set of even permutations. This is a normal subgroup, since for any $\sigma, \tau \in S_n$ we have

$$\operatorname{sgn}(\sigma\tau\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau).$$

We could have also noted that A_n is index 2 in S_n and applied Theorem 6.6 directly.

Example 6.8

Let D_{2n} be the dihedral group of order $2n$, and let H be the subgroup of n rotations. Then H is normal. On the other hand, the subgroup generated by a reflection is not normal.

Remark 6.9. Note that, as previously said, cosets partition the group, making a *smaller set* where the elements of those sets are collections of many group elements. However, the fact that normal subgroups form quotient *groups* makes this partition a group itself. This is why it is so useful; it helps with understanding the group in a simpler light.

§7 Lecture 7

In this section we will focus on examples of quotient groups.

Example 7.1

Let $G = S_n$ and $N = A_n$. There are exactly two left cosets of A_n in S_n: $1A_n, (1,2)A_n$, the latter consisting of all odd permutations. Hence the quotient S_n/A_n is cyclic of order 2.

Example 7.2

Consider the group S_4. The subgroup $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ is normal. The set $X = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$ is a *full set of left coset representatives of* V_4 *in* S_4, i.e. every coset of V_4 in S_4 contains exactly one element in X. This happens to be a subgroup of S_4, actually it's S_3. Hence we immediately identify the quotient group S_4/V_4 is isomorphic to S_3.

Example 7.3

Consider the group $\mathbb{Z}$ and the normal subgroup $n\mathbb{Z}$ for $n \in \mathbb{N}$. The quotient $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, n - 1 + n\mathbb{Z}\}$ is cyclic of order n, generated by $1 + n\mathbb{Z}$. This quotient group may be written as C_n.

§8 Lecture 8

§8.1 Group Homomorphisms, Types and Facts

Definition 8.1. Let G, G' be groups. A group homomorphism from G to G' is a function $\phi : G \to G'$ s.t. $\forall\ g, h \in G$ one has $\phi(gh) = \phi(g)\phi(h)$.

Remark 8.2. There is always at least one group homomorphism between any two groups, that is, the trivial homomorphism sending every element to the identity element.

Example 8.3

Write $\mathbb{R}^\times$ as the non-zero reals as a group under multiplication. For every $n \in \mathbb{N}$ we have the group homomorphism

$$\begin{aligned} \phi : \mathrm{GL}_n \mathbb{R} &\to \mathbb{R}^\times \\ X &\mapsto \det X \end{aligned}$$

where $\phi(XY) = \phi(X)\phi(Y)$.

Example 8.4

Let G be a group and N be a normal subgroup. The quotient map $G \to G/N$, sending $g \mapsto gN$, is a surjective group homomorphism. Note that the map is surjective because every coset will be mapped to, and homomorphism follows from the group operation of the quotient group. In particular, for every $n \in \mathbb{N}$ there is a surjective homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto k + n\mathbb{Z}$.

Remark 8.5. Note that in the definition of a homomorphism, we have two different multiplications going on: on the left hand side of the equation we use the group operation of G while on the right hand side we use the group operation of the co-domain G. The following is an example of this.

Example 8.6

The set $\mathbb{R}_{>0}$ is a group under multiplication. The map

$$\log : \mathbb{R}_{>0} \to \mathbb{R}, \quad x \mapsto \log x$$

is a homomorphism by the familiar property

$$\log xy = \log x + \log y.$$

Similarly, we have a homomorphism

$$\exp : \mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto e^x,$$

as

$$\exp(x + y) = \exp(x) \exp(y).$$

Notice that for each of the two homomorphisms a different operation is used on each side (multiplication and addition).

Theorem 8.7

Let $\phi : G \to G'$ be a group homomorphism. Then

1. $\phi(1_G) = 1_{G'}$, and
2. for every $g \in G$, $\phi(g^{-1}) = \phi(g)^{-1}$.

Proof. Let $g \in G$. Then $\phi(g) = \phi(1_G \cdot g) = \phi(1_G)\phi(g)$, and right multiplying by $\phi(g)^{-1}$ gives $\phi(1_G) = 1_{G'}$.
Furthermore, we have $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1_G) = 1_{G'}$, and symmetrically $\phi(g^{-1})\phi(g) = 1_{G'}$. Therefore, we have $\phi(g^{-1}) = \phi(g)^{-1}$, as required. □

The following theorem contains important results.

Theorem 8.8

We have the following

1. Let G, G', G'' be groups and $\phi : G \to G'$ and $\phi' : G' \to G''$ be group homomorphisms. Then the composition $\phi' \circ \phi : G \to G''$ form also a group homomorphism.
2. Let G be a group. The identity map $\phi : G \to G$, $g \mapsto g$ is a group homomorphism.
3. Let G, G' be groups, and define a bijective group homomorphism $\phi : G \to G'$. Then the inverse function $\phi^{-1} : G' \to G$ is also a group homomorphism.

Proof. Let $g, h \in G, g', h' \in G'$ throughout.
(1) Let $\omega = \phi' \circ \phi$ We have $\omega(gh) = \phi'(\phi(gh)) = \phi'(\phi(g)\phi(h)) = \phi'(\phi(g))\phi'(\phi(h)) = \omega(g)\omega(h)$. As required.

(2) We have $\phi(gh) = gh = \phi(g)\phi(h)$ as required.

(3) Without loss of generality define $\phi(g) = g'$ and $\phi(h) = h'$. We have $\phi(gh) = \phi(g)\phi(h) \iff gh = \phi^{-1}(\phi(g)\phi(h)) \iff \phi^{-1}(g')\phi^{-1}(h') = \phi^{-1}(g'h')$ as required. □

Remark 8.9 (Non-Examinable)**.** The first two statements are exactly what we need to show that groups form a category.

Definition 8.10. We define some common types of morphisms:

1. A group *isomorphism* is a group homomorphism $\phi : G \to G'$ that has a 2-sided inverse. This is, $\phi \circ \phi^{-1} = 1_{G'}, \phi^{-1} \circ \phi = 1_G$. If there exists a group isomorphism between groups G, G', we say these groups are isomorphic and write $G \cong G'$.
2. A group *endomorphism* is a group homomorphism from a group to itself.
3. A group *automorphism* is a group isomorphism from a group to itself.

Theorem 8.11

Let G, G' be groups and $\phi : G \to G'$ be group homomorphism. Then ϕ is an isomorphism if and only if ϕ is bijective.

Proof. If the homomorphism is an isomorphism, we have that it must have a two-sided inverse, and it follows that ϕ is bijective.

If ϕ is bijective, we claim that ϕ^{-1} exists and that it is a group homomorphism. This follows from Theorem 8.8. □

Remark 8.12. The significance of the notion of isomorphism is that two groups that are isomorphic are essentially structurally indistinguishable.

Example 8.13

All infinite cyclic groups are isomorphic to $\mathbb{Z}$.

A finite cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Theorem 8.14 (Cayley's theorem)

Every finite group G is isomorphic to a subgroup of the symmetric group $\mathrm{Sym}(G)$.

Proof. Let G be a group. For each $g \in G$, we associate a function $L_g : G \to G$ defined by $L_g(x) = gx$ for $x \in G$. This is clearly a permutation of G; it is a bijective function from G to G. Now let $\hat{G}$ be the set of all permutations L_g for all $g \in G$. In other words, $\hat{G} = \{L_g \mid g \in G\}$. We will now show that $\hat{G}$ is actually a subgroup of $\mathrm{Sym}(G)$. First, we have $L_e(x) = ex = x$, so L_e is the identity in $\hat{G}$. Let $g_1, g_2 \in G$. It is easy to see that $L_{g^{-1}}$ is the inverse of L_g. We have $(L_{g_1} \circ L_{g_2^{-1}})(x) = L_{g_1}(L_{g_2^{-1}}(x)) = g_1(g_2^{-1}x) = (g_1 g_2^{-1})x = L_{g_1 g_2^{-1}}(x) \in \hat{G}$. Therefore, $\hat{G}$ is a subgroup of $\mathrm{Sym}(G)$ by the subgroup test.

We finally show that G is isomorphic to $\hat{G}$; G is isomorphic to a subgroup of $\mathrm{Sym}(G)$. Consider the map,

$$\begin{aligned} \phi : G &\to \hat{G} \\ g &\mapsto L_g. \end{aligned}$$

We have

$$\phi(g_1g_2)(x) = L_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = L_{g_1}(L_{g_2}(x)) = \phi(g_1) \circ \phi(g_2)(x),$$

therefore the map is a homomorphism. The map is clearly injective and surjective, therefore $G \cong \hat{G}$. □

§9 Lecture 9

§9.1 First Isomorphism Theorem

Definition 9.1 (Kernel and Image)**.** Let $\phi : G \to G'$ be a group homomorphism.

Then the *kernel*, $\ker \phi$, is the set of all elements of G that are mapped to the identity of G', written as

$$\ker \phi = \{g \in G \mid \phi(g) = 1_{G'}\}.$$

The *image*, $\mathrm{Im}\, \phi$, is the set of all elements of G' mapped to under ϕ. Formally,

$$\mathrm{Im}\, \phi = \{\phi(g) \mid g \in G\}.$$

Theorem 9.2

Let $\phi : G \to G'$ be a group homomorphism. Then ϕ is injective if and only if $\ker \phi = \{1_G\}$, i.e. the kernel is trivial.

Proof. ($\implies$) Suppose ϕ is injective. Since ϕ is a homomorphism, $1_G \in \ker \phi$. If $k \in \ker \phi$, then

$$\phi(k) = 1_{G'} = \phi(1_G),$$

but ϕ is injective, so $k = 1_G$. Hence $\ker \phi$ is trivial.

($\impliedby$) Suppose $\ker \phi = \{1_G\}$ and suppose $\phi(g) = \phi(h)$. Then by properties of homomorphisms, $\phi(gh^{-1}) = 1_G$, so $gh^{-1} \in \ker \phi$, so $gh^{-1} = 1_G$, which means that $g = h$, so ϕ is injective. □

Remark 9.3 (Groups as symmetries, formalised)**.** If groups are thought of as symmetries, then homomorphisms are changes in the focus of attention of the same symmetry.

Example 9.4

Consider the dihedral group D_{12} of order 12. We can describe this by the presentation

$$D_{12} = \langle \sigma, \tau \mid \sigma^6 = \tau^2 = 1, \quad \sigma\tau = \tau\sigma^{-1} \rangle.$$

If we label the vertices of the hexagon as $1, 2, \ldots, 6$ we can view this dihedral group inside S_6, through its action on the set of vertices (see group actions). Then we observe how the rotation σ corresponds to (123456) and reflection τ to $(16)(25)(34)$, say. This is really saying that an injective group homomorphism $D_{12} \to S_6$ exists, defined by $\sigma \to (123456), \tau \to (16)(25)(34)$. This map should feel natural, as we are essentially just changing the focus from the symmetries of the whole hexagon to permutations of the vertices. We can realise D_{12} within S_6 in this way:

$$D_{12} = \langle (123456), (16)(25)(34) \rangle \leq S_6.$$

However, we can also consider the action of D_{12} on the set of diagonals of an hexagon. Then, for diagonals $1, 2, 3$, we have

$$\sigma \mapsto (123)$$

$$\tau \mapsto (13).$$

In other words, this action gives us a homomorphism $D_{12} \to S_3$, which is non-injective by the pigeonhole principle. Hence we must have a non-trivial element in the kernel, namely σ^3 which rotates 180 degrees, however in S_3 it gives back the identity. Although the homomorphism is non-injective, it is surjective.

Example 9.5

Recall that for a group G and N a normal subgroup of G, the quotient map, $\pi : G \to G/N$, $g \mapsto gN$, is a surjective homomorphism.

Let H. The inclusion map $\iota : H \to G$, $h \mapsto h$, is an injective group homomorphism.

Remark 9.6. Note that all isomorphisms are essentially a relabelling of the elements of the group.

This is the most important theorem of the course. The main use of this theorem is identify what groups a quotient is isomorphic to.

Theorem 9.7 (First isomorphism theorem, Part 1)

Let $\phi : G \to G'$ be a group homomorphism. Then

1. $\operatorname{Im}\phi \leq G'$,
2. $\ker\phi \trianglelefteq G$.

Proof. We first show that $\operatorname{Im}\phi$ is a subgroup of G. Note that $\operatorname{Im}\phi$ is nonempty since $\phi(1_G) = 1_{G'} \in \operatorname{Im}\phi$. Let $x, y \in \operatorname{Im}\phi$, then $\phi(g) = x$ and $\phi(h) = y$ for some $g, h \in G$. We have

$$xy^{-1} = \phi(g)(\phi(h))^{-1} = \phi(g)\phi(h^{-1}) = \phi(gh^{-1}) \in \operatorname{Im}\phi,$$

therefore, $\operatorname{Im}\phi$ is a subgroup by the subgroup test.

To prove that $\ker\phi \trianglelefteq G$, we will first show that it is indeed a subgroup. Note that $e_G \in \ker\phi$. Moreover, for $x, y \in \ker\phi$, we have $\phi(x) = \phi(y) = e_{G'}$. Therefore, $\phi(xy^{-1}) = \phi(x)(\phi(y))^{-1} = e_{G'}$, so $xy^{-1} \in \ker\phi$ and $\ker\phi$ is a subgroup of G by the subgroup test. Next, we claim that $\ker\phi$ is closed under conjugation by elements of G. Let $g \in G$ and $k \in \ker\phi$. We have,

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(gg^{-1}1) = e_{G'},$$

therefore, $gkg^{-1} \in \ker\phi$, as required. □

Our goal is now, given the kernel K of some homomorphism out of a group G, to understand the structure of the quotient group G/K.

Note that any homomorphism $\phi : G \to G'$ is surjective onto its image. In addition, ϕ may not be injective, but we can define an equivalence relation on G as

$$g \sim g' \iff \phi(g) = \phi(g') \iff gg^{-1} \in \ker\phi.$$

So if instead we modify the map to be a function on equivalence classes, this will be injective. We can think of this new map as placing the elements of G into boxes, represented by the different outputs of ϕ, and then mapping each box to this element of the image.

We have that K is a subgroup of G, so

$$g \sim g' \iff gg'^{-1} \in \ker\phi \iff gK = g'K.$$

So a function from the set of cosets, the quotient group, to the image of ϕ, sending gK to $\phi(g)$, will be both surjective and injective.

Theorem 9.8 (First Isomorphism Theorem)

Let $\phi : G \to G'$ be a group homomorphism. Then,

1. $\operatorname{Im}\phi \leq G'$,
2. $\ker\phi \trianglelefteq G$,
3. The mapping

$$\begin{aligned} \psi : G/\ker\phi &\to \operatorname{Im}\phi \\ g\ker\phi &\mapsto \phi(g) \end{aligned}$$

is a well-defined bijection. Moreover, it defines a group isomorphism,

$$G/\ker\phi \cong \operatorname{Im}\phi.$$

Proof. We proved statements 1 and 2 in Theorem 9.7. To prove the third statement, we first check that ψ is well-defined.

Let $g, g' \in G$ s.t. $g \ker\phi = g' \ker\phi$. Then we have $g = g'k$ for some $k \in \ker\phi$, and so $\phi(g) = \phi(g'k)$, therefore $\phi(g) = \phi(g')$. Hence we have that $g \ker\phi = g' \ker\phi \implies \phi(g) = \phi(g')$, i.e. ψ is well-defined.

To show that ψ is a homomorphism, let $g_1, g_2 \in G$. We have,

$$\psi(g_1 \ker\phi \cdot g_2 \ker\phi) = \psi(g_1 g_2 \ker\phi) = \phi(g_1 g_2) = \phi(g_1)\phi(g_2) = \psi(g_1 \ker\phi)\psi(g_2 \ker\phi),$$

since ϕ is a group homomorphism.

Furthermore, we claim that ψ is surjective and injective. Let $g' \in \operatorname{Im}\phi$, then $\exists g \in G$ s.t. $g' = \phi(g)$. We compute $\psi(g \ker\phi) = \phi(g) = g'$, therefore ψ is surjective.

Now suppose $g \in G$ s.t. $g \ker\phi \in \ker\psi$. We have $\psi(g \ker\phi) = \phi(g) = e$. Thus $g \in \ker\phi$ so $g \ker\phi = \ker\phi$ by absorption of cosets, meaning $\ker\psi$ is trivial and ψ is injective.

We have a bijective homomorphism and therefore an isomorphism. □

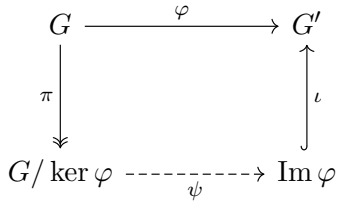


Figure 1: First isomorphism theorem, illustrated.

Remark 9.9. Every homomorphism is really a composition of a surjective quotient map and a bijective homomorphism from the quotient to the image.

§10 Lecture 10

On isomorphism theorems. The first isomorphism in action.

Proposition 10.1

A subgroup $H \leq G$ is normal if and only if H is the kernel of some homomorphism $\phi : G \to G'$.

Proof. Note that every kernel is a normal subgroup by the first isomorphism theorem. Conversely, if $N \trianglelefteq G$, we can define the quotient map $\phi : G \to G/N,\ g \mapsto gN$. This is a group homomorphism with kernel N since $\phi(g) = 1_{G/N} \iff gN = N \iff g \in N$. □

Remark 10.2. For a group G, it is essentially equivalent to list normal subgroups as it is to list group homomorphisms out of G.

Definition 10.3. Let $(H, *), (K, \cdot)$ be groups. We define their *direct product* as the group with underlying set $H \times K = \{(h, k) : h \in H, k \in K\}$ with operation of point-wise multiplication $(h, k)(h', k') = (h * h', k \cdot k')$.

Proposition 10.4

Let H and K be groups, and let $G = H \times K$. The subset $H \times \{1_K\}$ is a normal subgroup of G isomorphic to H, and one has $G/H \times \{1_K\} \cong K$. Similarly, $\{1_H\} \times K$ is a normal subgroup of G isomorphic to K, and one has $G/\left(\{1_H\} \times K\right) \cong H$.

Proof. Consider the map

$$\phi : H \times \{1_K\} \to H$$

defined by $\phi((h, 1)) = h$. This is clearly an isomorphism. Now consider the canonical projection map

$$\pi : H \times K \to K$$

defined by $\pi((h, k)) = k$. Then $\ker \pi = \{(h, 1_K) : h \in H\} = H \times 1_K$. Since kernels are normal subgroups, we have shown that $H \times /1_K$ is a normal subgroup of G. We have $\operatorname{Im} \pi = K$ trivially. Therefore, by the FIT, we have $H \times K/H \times \{1_K\} \cong K$, or equivalently, $G/H \times 1_K \cong K$. Similarly, we have $\{1_H\} \times K \cong K$, is a normal subgroup of G, and $G/\left(\{1_H\} \times K\right) \cong H$. □

Example 10.5

We have previously seen (Example 9.4) that there exists a homomorphism from D_{12} to S_3. The kernel of this homomorphism is the subgroup H generated by the rotation by 180^o, and the image is all of S_3. By FIT, we have $D_{12}/H \cong S_3$.

Example 10.6

Let $\mathbb{C}^\times$ be the non-zero complex numbers as a group under multiplication. The function $f : \mathbb{R} \to \mathbb{C},\ x \mapsto e^{2\pi i x}$ is a group homomorphism. The image is the unit circle in $\mathbb{C}$, denoted S^1, and the kernel is $\mathbb{Z}$. Then,

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

This can be extended to show that

$$\mathbb{R}^n/\mathbb{Z}^n \cong \bigoplus_{i=1}^{n} S^1.$$

Example 10.7

Consider the homomorphism from $\mathbb{C}^\times$ to $\mathbb{R}_{>0}$ viewed as groups under multiplication given by $z \mapsto |z|$. The image is $\mathbb{R}_{>0}$ and the kernel is S^1. Hence by FIT,

$$\mathbb{C}^\times/S^1 \cong \mathbb{R}_{>0}$$

Example 10.8

How many distinct homomorphisms $\phi : G \to G'$ are there from $G = C_4 = \langle g \mid g^4 = 1\rangle$ to $G' = C_{10} = \langle g' \mid (g')^{10} = 1\rangle$?

We will begin by listing our options for possible kernels and images, and then classify our homomorphisms by the choices of kernel. First note that since G is cyclic, it is abelian and therefore all of its subgroups are normal and can be kernels of the map.

The group G has three subgroups: the trivial subgroup $\{e\}$, the subgroup $\langle g^2\rangle = \{e, g^2\}$, and the group itself, G.

Our options for image are subgroups of G'. We have: $\{e\}$, $\langle (g')^5\rangle = \{e, (g')^5\}$, and the group itself, G'.

Now consider a map ϕ with $\ker\phi = \{e\}$. By FIT, we must have $G/\{e\} \cong G \cong \operatorname{Im}\phi$, but G' has no subgroup of order 4, so there is no such map.
Now consider ϕ with $\ker\phi = \{e, g^2\}$. Again, by FIT, we must have $C_4/\{1, g^2\} = \{\{1, g^2\}, \{g, g^3\}\} \cong \operatorname{Im}$. We can take $\operatorname{Im}\phi = \{e, (g')^5\}$.
Finally, consider $\ker\phi = G$. We must have $G/G \cong \{e\} \cong \operatorname{Im}\phi$. We can take $\operatorname{Im}\phi = \{e\}$, and this is in fact the trivial homomorphism sending every element to the identity in G'.
Therefore, there are only two possible homomorphisms.

§11 Lecture 11

§11.1 Second Isomorphism Theorem

Theorem 11.1 (Second Isomorphism Theorem)

Let G be a group, $H \leq G$, $N \trianglelefteq G$. Then,

1. $HN = \{hn \mid h \in H, n \in N\} \leq G$,
2. $H \cap N \trianglelefteq H$,
3. $H/H \cap N \cong HN/N$.

Proof. (1) We will start by showing that $HN = NH$. Let $hn \in HN$. Since $N \trianglelefteq G$, $hnh^{-1} \in N$, so there exists $n' \in N$ such that $hnh^{-1} = n'$. Therefore $hn = n'h$, so $HN \subset NH$. It can be shown similarly that $NH \subset HN$, so $HN = NH$.

We now show that HN is a subgroup of G by the subgroup test. We have $1_G \in HN$, so HN is nonempty. Now let $x = h_1n_1 \in HN$ and $y = h_2n_2 \in HN$. Then

$$xy^{-1} = (h_1n_1)(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1}.$$

As we have shown $HN = NH$, we can write $n_2^{-1}h_2^{-1} = \hat{h}\hat{n}$ for some $\hat{h}\hat{n} \in HN$, so

$$xy^{-1} = h_1n_1\hat{h}\hat{n}.$$

Again, we can write $n_1\hat{h} = \tilde{h}\tilde{n}$ for some $\tilde{h}\tilde{n} \in HN$, so

$$xy^{-1} = h_1\tilde{h}\tilde{n}\hat{n} \in HN,$$

as required.

(2) We want to show $H \cap N$ is closed under conjugation by elements of H. Let $h \in H$ and $x \in H \cap N$, i.e. $x \in H$ and $x \in N$. We have $hxh^{-1} \in H$ as H is a group. Also, since $N \trianglelefteq G$, $hxh^{-1} \in N$. Therefore, $hxh^{-1} \in H \cap N$, as required.

(3) We define

$$\begin{array}{rccccc} \varphi: & H & \hookrightarrow & G & \to & G/N \\ & \cup & & & & \cup \\ & h & \longmapsto & & & hN. \end{array}$$

Since φ is the composition of an inclusion map and a natural projection, which are both homomorphisms, it is also a homomorphism.

We have that $\ker \varphi = \{h \in H \mid \varphi(h) = N\} = \{h \in H \mid h \in N\} = H \cap N$.

Also,

$$\begin{aligned} \operatorname{Im} \varphi &= \{\varphi(h) \mid h \in H\} \\ &= \{gN \mid gN = \varphi(h) \text{ for some } h \in H\} \\ &= \{gN \mid gN = hN \text{ for some } h \in H\} \\ &= \{gN \mid h^{-1}g \in N, h \in H\} \\ &= \{gN \mid g \in HN\} \\ &= HN/N. \end{aligned}$$

Hence, by the first isomorphism theorem,

$$H/H \cap N \cong HN/N.$$

□

Example 11.2

Let $\mathrm{GL}_2(\mathbb{R})$ be the multiplicative group of invertible 2×2 matrices over $\mathbb{R}$. Let $SL_2(\mathbb{R}) \leq \mathrm{GL}_2(\mathbb{R})$ be the subgroup of matrices with determinant 1. This is a normal subgroup. What is the structure of $\mathrm{GL}_2(\mathbb{R})/SL_2(\mathbb{R})$?

By the first isomorphism theorem we have that $\mathrm{SL}_2(\mathbb{R})$ must be the kernel of some group homomorphism, namely the determinant map. The image of the determinant is all $\mathbb{R}^\times$, so we deduce that $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R}) \cong \mathbb{R}^\times$.

Consider the subgroup

$$Z = \left\{\operatorname{diag}(a, a) \mid a \in \mathbb{R}^\times\right\} \leq \mathrm{GL}_2(\mathbb{R})$$

of diagonal matrices. We wish to understand Z in the context of $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R})$ using the SIT. Observe that $\operatorname{diag}(a, a) \in Z$ has determinant a^2, so we see that $Z \cap \mathrm{SL}_2(\mathbb{R}) = \{\pm \operatorname{diag}(1, 1)\}$, a group consisting of 2 elements.

The remaining component of the SIT to understand is $Z \cdot \mathrm{SL}_2(\mathbb{R})$. We claim without proof this is $\mathrm{GL}_2^+(\mathbb{R}) = \{X \in \mathrm{GL}_2(\mathbb{R}) \mid \det(X) > 0\}$.

Applying the SIT with $H = Z$ and $N = \mathrm{SL}_2(\mathbb{R})$, we have

$$Z/\{\pm \operatorname{diag}(1, 1)\} \cong \mathrm{GL}_2^+(\mathbb{R})/\mathrm{SL}_2(\mathbb{R}) \cong \mathbb{R}_{>0}.$$

§11.2 Non-examinable aside

To explain how SIT will be useful eventually, we introduce the idea of *atoms of group theory*. If we want to understand a big and complicated group G, we can do so by finding a normal subgroup N and understanding its quotient G/N (which is in essence a group with similar structure to G but with less elements). Note that this reduction step relies on the existence of a proper non-trivial normal subgroup. The SIT is very useful in this approach.

Definition 11.3 (Simple Group)**.** A group is *simple* if it is non-trivial and has no proper non-trivial normal subgroups.

If we understand all simple groups, and how bigger groups are made up of smaller simple groups and their quotients, we would understand all groups. All finite simple groups have been classified.

Definition 11.4. A group G is called *metabelian* if it has a normal subgroup N such that both N and G/N are abelian.

Theorem 11.5

Let G be a metabelian group. Then every subgroup of G is also metabelian.

Proof. Let G be metabelian, let N be a normal subgroup such that N and G/N are abelian, and let H be an arbitrary subgroup of G. We claim that H is also metabelian. Indeed, $H \cap N$ is a normal subgroup of H, and it is abelian, since it is a subgroup of the abelian group N; moreover, by SIT we have $H/(H \cap N) \cong HN/N \leq G/N$, so $H/(H \cap N)$ is abelian, being (isomorphic to) a subgroup of an abelian group. Thus $H \cap N$ is the required normal subgroup of H. □

§12 Lecture 12

On the 3rd isomorphism theorem.

§12.1 Third Isomorphism Theorem

Lemma 12.1

Let $\phi : G \to G'$ be a homomorphism and $H' < G'$. We claim that the preimage $\phi^{-1}(H') < G$ is a subgroup of G.

Proof. Since H' is a subgroup of G', we have $1_{G'} \in H'$, so $\phi(1_G) = 1_{G'}$ and it follows that $1_G \in \phi^{-1}(H')$. Let $x, y \in \phi^{-1}(H')$, then we have that $x = \phi^{-1}(h')$, $y = \phi^{-1}(h)$ for some $h, h', \in H'$, or equivalently, $h' = \phi(x)$ and $h = \phi(y)$. It follows that

$$h'h^{-1} = \phi(x)\phi(y)^{-1} = \phi(xy^{-1}) \in H',$$

therefore $xy^{-1} \in \phi^{-1}(H')$, as required. □

Theorem 12.2 (Third Isomorphism Theorem)
If N and K are normal in G with $N \subseteq K$, then we have an isomorphism of groups $G/K \cong (G/N)/(K/N)$.

Proof. We claim that $\widetilde{f} : G/K \to (G/N)/(K/N)$, defined by $gK \mapsto gN(K/N)$, is an isomorphism of groups. First, to check the map is well defined, suppose $gK = g'K$ for some $g, g' \in G$. We have,

$$\begin{aligned} gK = g'K &\iff g^{-1}g' \in K \\ &\iff g^{-1}g'N \in K/N \\ &\iff gN(K/N) = g'N(K/N), \end{aligned}$$

as required. The equivalences above read backwards give us the injectivity of $\widetilde{f}$.

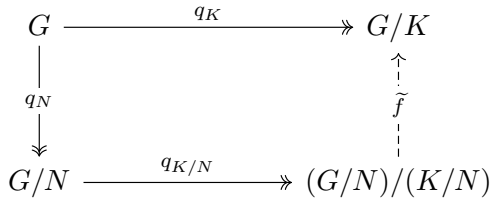
The map is clearly surjective; for all $gN(K/N) \in (G/N)(K/N)$, we have $gK \in G/K$ with $\widetilde{f}(gK) = gN(K/N)$.

We are left to prove that $\widetilde{f}$ is a homomorphism. We have

$$\begin{aligned} \widetilde{f}(gKg'K) = \widetilde{f}(gg'K) &= gg'N(K/N) \\ &= gN(K/N)g'N(K/N) = \widetilde{f}(gK)\widetilde{f}(g'K). \end{aligned}$$

We have a bijective homomorphism and therefore an isomorphism. □

This is easier to understand with the following commutative diagram:



Remark 12.3. The third isomorphism theorem says that the quotient homomorphism $q_K : G \to G/K$ can be factored through the quotient homomorphism $q_N : G \to G/N$ to give $q_K \simeq q_{K/N} \circ q_N$.

An intuitive way of thinking about the 3rd Isomorphism Theorem is as follows: suppose that G is a group, K is a normal subgroup, and $\phi : G \to G'$ is a group homomorphism to some other group G' whose kernel $N = \ker \phi$ is contained in K. Then the kernel of ϕ restricted to K is still N. By FIT, ϕ induces isomorphisms $G/N \cong \phi(G)$ and $K/N \cong \phi(K)$. It can be shown that the 3rd Isomorphism Theorem is saying that one has an isomorphism

$$G/K \cong \phi(G)/\phi(K).$$

It is not true in general that $G \cong G'$ and $N \cong N'$ implies $G/N \cong G'/N'$ (see ex sheet 3 Q14); there is something to prove here. We need to show that for G, K, N as defined above, we have $(G/N)/(K/N) \cong \phi(G)/\phi(K)$. Consider the map

$$\psi : \phi(G) \to (G/N)/(K/N)$$

defined by $\phi(g) \mapsto gN(K/N)$. This map is clearly surjective; for any $gN(K/N)$, we have $\phi(g) \in \phi(G)$, so we have $\psi(\phi(g)) = gN(K/N)$. Now,

$$\begin{aligned}\ker \psi &= \{\phi(g) \mid \psi(\phi(g)) = K/N\} \\ &= \{\phi(g) \mid gN(K/N) = K/N\} \\ &= \{\phi(g) \mid gN \in K/N\} \\ &= \{\phi(g) \mid g \in K\} = \phi(K).\end{aligned}$$

Therefore, by the first isomorphism theorem, we have $\phi(G)/\phi(K) \cong (G/N)/(K/N)$, and by the third isomorphism theorem, $G/K \cong (G/N)/(K/N) \cong \phi(G)/\phi(K)$, as required.

In other words, if we want to understand some quotient G/K, then we may apply any homomorphism ϕ to G whose kernel is contained in K, and it suffices to understand the quotient "on the other side" of ϕ.

Example 12.4

Let $G = \mathrm{GL}_2(\mathbb{R})$ and let $K = \mathrm{GL}_2^+(\mathbb{R}) = \{X \in \mathrm{GL}_2(\mathbb{R}) : \det X > 0\}$. It is easy to see that K is closed under conjugation by elements of G, so K is normal in G. We want to study G/K using the Third Isomorphism Theorem. We have $N = \mathrm{SL}_2(\mathbb{R}) \subset K$, and $N \trianglelefteq G$ as it is the kernel of the determinant map. Consider the surjective group homomorphisms $\det : G \to \mathbb{R}^\times$ and $\det : \mathrm{GL}_2^+(\mathbb{R}) \to \mathbb{R}_{>0}$. Both have kernel N, so by the FIT we have $G/N \cong \mathbb{R}^\times$ and $K/N \cong \mathbb{R}_{>0}$. Now, by the 3rd Iso. Thm. we have $G/K \cong \det \mathrm{GL}_2(\mathbb{R}) / \det \mathrm{GL}_2^+(\mathbb{R}) \cong \mathbb{R}^\times/\mathbb{R}_{>0} \cong \{\pm 1\}$.

Lemma 12.5

Let G be a group and $N \trianglelefteq G$. Then every subgroup U of G/N is of the form H/N for some $H \leq G$ containing N.

Proof. Let $H = \pi^{-1}(U)$. By Lemma 12.1, $H \leq G$. Furthermore, because $N = 1_{G/N} \subseteq U$, we have $\pi^{-1}(N) = N \subseteq H$. Hence, the quotient H/N is well defined.

We go by way of double inclusion.

$(H/N \subseteq U)$ Let $hN \in H/N$. As $H = \pi^{-1}(U)$, we have $\pi(h) = hN \in U$.

$(U \subseteq H/N)$ Let $u \in U$, then $u = gN$ for some $g \in G$. Since $gN \in U, \pi(g) \in U$, so $g \in H$ and thus $u \in H/N$.

So every subgroup of G/N is of the form H/N. □

Theorem 12.6 (Correspondence Theorem)

Let G be a group, let N be a normal subgroup, and let π be the quotient map $G \to G/N$. Then:

1. For subgroup U of G/N the assignment $U \mapsto \pi^{-1}(U)$ defines a bijection between the set of subgroups of G/N and the set of those subgroups of G that contain N;
2. The above assignment defines a bijection between the set of normal subgroups of G/N and the set of normal subgroups of G containing N.

Proof. (1) Let $\mathcal{S}_N^G$ denote the set of all subgroups of G that contain N, and let $\mathcal{S}^{G/N}$ denote the set of subgroups of G/N. We know from Lemma 12.5 that every element of $\mathcal{S}^{G/N}$ is of the form H/N. So we have our pre-image map $\pi^{-1} : \mathcal{S}^{G/N} \to \mathcal{S}_N^G$ defined by $H/N \mapsto \{g \in G \mid gN \in H/N\} = H \leq G$, by Lemma 12.1. We claim that the map $\theta : \mathcal{S}_N^G \to \mathcal{S}^{G/N}$ defined by $H \mapsto H/N$ is the inverse of π^{-1}.

To show that θ is the right inverse, we have that $\pi^{-1}(\theta(H)) = \pi^{-1}(H/N) = \{g \in G \mid gN \in H/N\} = H$, so $\pi^{-1} \circ \theta = \mathrm{id}_{\mathcal{S}_N^G}$, the identity map on $\mathcal{S}_N^G$.

Now for the left inverse, we have $\theta(\pi^{-1}(H/N)) = \theta(\{g \in G \mid gN \in H/N\}) = \theta(H) = H/N$, so $\theta \circ \pi^{-1} = \mathrm{id}_{\mathcal{S}^{G/N}}$, the identity map on $\mathcal{S}^{G/N}$.

Thus, there is a bijection between $\mathcal{S}^{G/N}$ and $\mathcal{S}_N^G$.

(2) From sheet 2, q5, since π is a surjective homomorphism, we have that $\pi^{-1}(U)$ is a normal subgroup of G if and only if U is normal in G/N. Note that because U is a subgroup of G/N, $\pi^{-1}(U)$ contains N. Hence every normal subgroup of G containing N has an associated normal subgroup of G/N and vice versa, i.e. there is a bijection between these two sets. □

§13 Lecture 13

§13.1 Group Actions

Group actions are in a way the birth of groups; the notion of a group action came before the notion of an abstract group.

Definition 13.1 (Left action)**.** Let G be a group, and let X be a set. A *left action* of G on X is a function

$$G \times X \to X$$

$$(g, x) \mapsto g \cdot x \in X$$

such that

1. $1_G \cdot x = x$ for any $x \in X$, and
2. $g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x$ for any $g_1, g_2 \in G$ and $x \in X$.

> **Remark 13.2.** In the second property above, the $\cdot$ symbol in the bracket on the right hand side denotes the group operation, while all the other "multiplications" in that equality are the actions of G on X.

Definition 13.3 (Right action)**.** Analogously, a *right action* of a group G on a set X is a function

$$X \times G \to X$$

$$(x, g) \mapsto x \cdot g$$

Such that

1. for all $x \in X$ one has $x \cdot 1_G = x$, and
2. for all $g_1, g_2 \in G$ and for all $x \in X$ one has $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 \cdot g_2)$.

Remark 13.4. Note that in a left action, first acting by g_2 and then acting on the result by g_1 is the same as acting by the product g_1g_2. For a right action, first acting by g_2 and then by g_1 is the same as acting by the product g_2g_1. In other words, right and left actions are not the same.

Definition 13.5. A set X equipped with an action by a group G is called a G-set.

Theorem 13.6

Let G be a group and X a G-set. Then

1. For every $g \in G$, the function $\sigma_g : X \to X$ given by $x \mapsto g \cdot x$ is injective. In other words, every $g \in G$ induces a permutation of X.
2. The function $\phi : G \to \mathrm{Sym}(X)$ given by $g \mapsto \sigma_g$ is a group homomorphism.

Proof. To prove the first claim, we have $\sigma_g(x) = \sigma_g(y) \implies g \cdot x = g \cdot y \implies (g^{-1}g) \cdot x = (g^{-1}g) \cdot y \implies 1_G \cdot x = 1_G \cdot y \implies x = y$.

The second claim follows by the second axiom in Definition 13.1. Let $\mathrm{Sym}(X)$ be the set of permutations of X. Let $g, g' \in G$ and $x \in X$. Then $\phi(gg')(x) = \sigma_{gg'}(x) = (gg') \cdot x = g \cdot (g' \cdot x) = g \cdot (\sigma_{g'}(x)) = \sigma_g(\sigma_{g'}(x)) = \phi(g)\phi(g')$, as required. □

As we have just seen, every $g \in G$ induces a permutation of X, so we can think of group actions in another way. The following is the 2F definition of a group action.

Definition 13.7. A group G is said to act on a set X if there exists a group homomorphism

$$\phi : G \to \mathrm{Sym}(X).$$

Given such a homomorphism ϕ, then we say an element $g \in G$ acts on X by sending an element $x \in X$ to the element $g \cdot x$ defined by

$$g \cdot x = \phi(g)(x).$$

Example 13.8

Let $n \in \mathbb{N}$. The group S_n acts on $\{1, \ldots, n\}$.

For $n \in \mathbb{N}_{\geq 3}$, the dihedral group of order $2n$ acts on the set of vertices and also on the set of edges of a regular n-gon. Moreover, if n is even, it acts on the set of diagonals.

Example 13.9

Let G be the group of symmetries of a cube. Then G acts on the set of diagonals of the cube. We can label each diagonal of the cube 1, 2, 3 and 4, and any symmetry of the cube will permute these labels. Let us consider all the symmetries of a cube (you may want to view this webpage to help with the visualisation of this).

First, consider the axis of symmetry through a face of the cube. We have an element of order two, rotation by π. We have two elements of order four, rotation by $\frac{\pi}{2}$ and $\frac{3\pi}{2}$. Since we have three opposite face pairs, we calculate 3(2+1)= 9 elements constituting symmetries about an axis through opposite faces.

Next, we consider the axis of symmetry through the midpoints of a pair of opposite edges. We have one element of order two, rotation by π. Since we have 6 opposite edge pairs, we have 6 such elements.

Finally, we consider the axis of symmetry through a pair of opposite vertices. We have two elements of order three, rotation by $\frac{2\pi}{3}$ and $\frac{4\pi}{3.}$ We have four opposite vertex pairs, and therefore 8 such elements.

In total, we have 6+8+9=23 non-identity elements, so G is isomorphic to a group of order 24. By considering the orders of the elements we've counted above (6 elements of order 4, 8 of order 3, etc...), we see that this group is in fact S_4.

Definition 13.10. Let G be group acting on a set X. That is, we have a group homomorphism $\phi : G \to \mathrm{Sym}(X)$. We say that this is a *faithful* group action if the homomorphism ϕ is injective.

What this is saying is that the action "faithfully" represents the symmetries of the group. That is no two elements $g, g' \in G$ are mapped to the same permutation $\sigma \in \mathrm{Sym}(X)$. A faithful action embeds the group structure into the symmetries of the set X. Each group element corresponds to a unique permutation of X, and observing how the set X is transformed reveals the group element responsible for that action. This means that the action of the group on the set effectively "encodes" the group's structure.

Example 13.11

Consider the usual action of $G = S_3$ on the set $X = \{1, 2, 3\}$. This is a faithful group action.

Define an action of $G = S_3$ on the set $X = \{x\}$ by the formula $\sigma \cdot x = x$ for all $\sigma \in S_3$. This is NOT a faithful group action.

Remark 13.12. Note that with non-faithful actions we "lose information" about the group. If we think of groups as encoding the symmetries of an object, then in this situation we have not made a suitable choice of set for our group to act on in order to preserve all of the information.

The following is a proof of Cayley's Theorem again, however this time using the new tools we have developed. You should compare this with the first proof in lecture 9.

Theorem 13.13 (Cayley's Theorem)

Every finite group G is isomorphic to a subgroup of the symmetric group $\mathrm{Sym}(G)$.

Proof. Let G be a group. Then we can view G itself as a G-set through the action of left multiplication

$$L : G \to \mathrm{Sym}(G)$$

defined by $L(g)(h) = gh$. We claim this action is faithful; this is equivalent to Cayley's theorem as our action being faithful means our group homomorphism L is injective, meaning there is an isomorphism between G and $\mathrm{Im}\, L \leq \mathrm{Sym}(G)$.

Checking that L is a group action is straightforward. Let us check that it is faithful. Suppose $g \in \ker L$. That mean $L(g)$ is the identity element of $\mathrm{Sym}(G)$, that is $L(g)(h) = h$ for all $h \in G$. Since $L(g)(h) = gh$ by definition of L, we have $gh = h$ for all $h \in G$. Therefore g must be the identity element of G. So $\ker L = \{1_G\}$, i.e. the homomorphism L is injective. So the action is faithful. □

Definition 13.14. Let G be a group. A G-action on a set X is called *transitive* if for any $x, y \in X$ there exists $g \in G$ s.t. $y = g \cdot x$.

Example 13.15

Let G be a group and H be a subgroup. The set of left cosets of H in G is a transitive G-set under the action

$$\begin{aligned} G \times G/H &\to G/H \\ (g, xH) &\mapsto (gx)H. \end{aligned}$$

It is easy to check this action is well defined, transitivity is also simple: given any two left cosets $xH, yH \in G/H$, we want to find $g \in G$ such that $g \cdot (xH) = yH$. One can see that taking $g = yx^{-1}$ completes the proof.

Definition 13.16 (Isomorphism on group action)**.** Let G be a group and X, Y be G-sets. A G-set *isomorphism* from X to Y is a bijection $\phi : X \to Y$ s.t. $\forall x \in X, g \in G$, we have $\phi(g \cdot x) = g \cdot \phi(x)$.

Theorem 13.17

Let G be a group and let H, K be subgroups. Then the G-sets G/H and G/K are isomorphic if and only if there exists $g \in G$ such that $H = gKg^{-1}$.

Proof. Note that we need to be clever with how we define our G-set isomorphism, the map $f : G/H \to G/K$ defined by $gH \mapsto gK$ is not a G-set isomorphism as it fails to preserve the action, that is $h \cdot f(H) = hK \neq H = f(hH)$ for $h \in H$.

($\Longleftarrow$) Assume H and K are conjugate, so there exists $g \in G$ such that $H = gKg^{-1}$. Define a map $\phi : G/H \to G/K$ by $\phi(xH) = xgK$. This map is well-defined because if $xH = yH$ for $x, y \in G$, then $y^{-1}x \in H = gKg^{-1}$, and so $g^{-1}y^{-1}xg \in K$. It follows that $ygK = xgK$, hence $\phi(xH) = \phi(yH)$.

To show that ϕ is a G-set isomorphism, we need to prove that it is bijective and respects the G action. For bijectivity, define a map $\psi : G/K \to G/H$ by $\psi(xK) = xg^{-1}H$. By a similar argument to that above, ψ is well-defined and it is easily seen that ψ is the inverse of ϕ.

To show that ϕ respects the G action, let $g' \in G$ and $xH \in G/H$. Then $\phi(g' \cdot xH) = \phi(g'xH) = g'xgK$. Since $g'xH = g'(xH)$, we have $g'xgK = g' \cdot \phi(xH)$. Hence, ϕ respects the G action, and so G/H and G/K are isomorphic as G-sets.

($\implies$) Conversely, assume the G-sets G/H and G/K are isomorphic. This means there exists a bijective function $f : G/H \to G/K$ that also respects the G action; that is, for all $g \in G$ and $xH \in G/H$, we have $f(g \cdot xH) = g \cdot f(xH)$. Consider $f(1_G \cdot H) = gK$ for some $g \in G$. Since f respects the G action, for any $h \in H$, we have $f(h \cdot H) = h \cdot f(H) = h \cdot gK$. Since $hH = H$, it follows that $hgK = gK$ and so $g^{-1}hg \in K$. This shows that $H \subseteq gKg^{-1}$.

To show the other inclusion, consider the inverse isomorphism $f^{-1} : G/K \to G/H$. We have $f^{-1}(1_G \cdot K) = g^{-1}H$ for some $g^{-1} \in G$. By a similar argument as above, for any $k \in K$, we have $g^{-1}kg \in H$, which shows that $K \subseteq g^{-1}Hg$. Thus, $H = gKg^{-1}$, and H and K are conjugate.

Therefore, G/H and G/K are isomorphic G-sets if and only if H and K are conjugate subgroups. □

§14 Lecture 14

§14.1 Orbit-Stabiliser Theorem

Definition 14.1 (Orbit and Stabiliser)**.** Let G be a group and X be a G-set. Let $x \in X$. The *orbit* of x under the action of G is $\mathrm{Orb}_G(x) = G \cdot x = \{g \cdot x \mid g \in G\}$. The *stabiliser* of x in G is $\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$.

Theorem 14.2

Let G be a group and X be a G-set, and let $x \in X$. Then

1. The G-orbit of x is a transitive G-set,
2. The stabiliser of x is a subgroup of G.

Proof. (1) We have to show that $\mathrm{Orb}_G(x)$ is indeed a G-set and that it is transitive. Let $\tilde{x} \in G \cdot x$, then $\tilde{x} = g \cdot x$ for some $g \in G$. We now check the two axioms for a group action. First,

$$1_G \cdot \tilde{x} = 1_G \cdot (g \cdot x) = (1_G \cdot g) \cdot x = g \cdot x = \tilde{x},$$

where the equalities follow from X being a G-set.

Now for the second axiom, let $g_1, g_2 \in G$. We check,

$$g_1 \cdot (g_2 \cdot \tilde{x}) = g_1 \cdot (g_2 \cdot g \cdot x) = (g_1 \cdot g_2) \cdot g \cdot x = (g_1 \cdot g_2) \cdot \tilde{x},$$

as required.

Moreover, we claim that the G-orbit of x is transitive, that is, for all $\tilde{x}, \tilde{y} \in G \cdot x$, there exists some $g \in G$ such that $\tilde{y} = g \cdot \tilde{x}$. We have $\tilde{x} = g_1 \cdot x$, $\tilde{y} = g_2 \cdot x$ for some g_1, $g_2 \in G$. It follows that

$$\tilde{y} = g_2 \cdot x = g_2 \cdot (g_1^{-1} \cdot (g_1 \cdot x)) = (g_2 g_1^{-1}) \cdot \tilde{x},$$

as required.

(2) We now show that the stabiliser is indeed a subgroup. We clearly have $1_G \in \mathrm{Stab}_G(x)$, so the set is non-empty. Let $g_1, g_2 \in \mathrm{Stab}_G(x)$, so $g_1 \cdot x = g_2 \cdot x = x$. From the first equality we have $(g_2^{-1}g_1) \cdot x = x$, so $g_2^{-1}g_1 \in \mathrm{Stab}_G(x)$, meaning $\mathrm{Stab}_G(x)$ is a subgroup by the subgroup test. □

Theorem 14.3 (Orbit-Stabiliser Theorem)

Let G be a group and X be a G-set. Let $x \in X$. Then there is an isomorphism of G-sets given by

$$\begin{aligned} \phi : G/\operatorname{Stab}_G(x) &\to \operatorname{Orb}_G(x) \\ g\operatorname{Stab}_G(x) &\mapsto g \cdot x. \end{aligned}$$

Proof. We must check that ϕ is well defined and a G-set isomorphism.

Let $g, g' \in G$ and suppose $g\,\mathrm{Stab}_G(x) = g'\,\mathrm{Stab}_G(x)$. Then $g^{-1}g' \in \mathrm{Stab}_G(x)$, so $(g^{-1}g') \cdot x = x$. Acting on the left by g, we see that

$$g' \cdot x = (gg^{-1}g') \cdot x = g \cdot (g^{-1}g') \cdot x = g \cdot x,$$

so ϕ is well defined.

Now for injectivity, suppose $\phi(g\,\mathrm{Stab}_G(x)) = \phi(g'\,\mathrm{Stab}_G(x))$. This means $g \cdot x = g' \cdot x$, and we can apply the above logic in reverse to conclude that $g\,\mathrm{Stab}_G(x) = g'\,\mathrm{Stab}_G(x)$, so ϕ is injective.

Let $y \in \mathrm{Orb}_G(x)$, then $\exists g \in G$ s.t. $y = g \cdot x$. Then $\phi(g\,\mathrm{Stab}_G(x)) = g \cdot x = y$, so ϕ is surjective.

Finally, to prove ϕ is a G-set isomorphism, let $g, h \in G$. We want to show that $g \cdot (\phi(h\,\mathrm{Stab}_G(x))) = \phi(g \cdot (h\,\mathrm{Stab}_G(x)))$.

We have that

$$\begin{aligned} g \cdot (\phi(h\operatorname{Stab}_G(x))) &= g \cdot (h \cdot x) \\ &= (gh) \cdot x \\ &= \phi(gh\operatorname{Stab}_G(x)) \\ &= \phi(g \cdot (h\operatorname{Stab}_G(x))), \end{aligned}$$

as required. □

Corollary 14.4

Let G be a group and X be a G-set. Let $x \in X$. We have $|\operatorname{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)]$. In particular, if G is finite, then $|\operatorname{Orb}_G(x)| = |G|/|\operatorname{Stab}_G(x)|$, by Lagrange, and the size of every orbit divides $|G|$.

Proof. Let ϕ be as in the statement of Theorem 14.3. Since ϕ is a bijection, we have $|\operatorname{Orb}_G(x)| = |G/\operatorname{Stab}_G(x)| = [G : \mathrm{Stab}_G(x)]$. If G is finite Lagrange's Theorem says $|G| = |\operatorname{Stab}_G(x)| \cdot |\operatorname{Orb}_G(x)|$, so the size of the orbit of x divides $|G|$. □

Theorem 14.5

Let G be a group and X be a G-set. Then lying in the same orbit is an equivalence relation on X. In particular, X is a union of disjoint orbits (equivalence classes).

Proof. We have that $x \sim y \iff \exists g \in G$ s.t. $g \cdot x = y$.

The relation is reflexive since $1_G \cdot x = x$.

If $x \sim y$, then $\exists g \in G$ s.t. $g \cdot x = y \implies g^{-1} \cdot y = x$, so $y \sim x$ and the relation is symmetric.

If $x \sim y$ and $y \sim z$, then $\exists g, g' \in G$ s.t. $g \cdot x = y$ and $g' \cdot y = z$. Then $((g'g) \cdot x) = z$, so $x \sim z$ and the relation is transitive. □

Theorem 14.6

Let G be a group, and let X be a transitive G-set. Then any two point stabilisers are conjugate in G. That is, for any $x, y \in X$ there exists $g \in G$ with $\mathrm{Stab}_G(x) = g\,\mathrm{Stab}_G(y)g^{-1}$.

Proof. Let $x, y \in X$. Since X is transitive, there is a $g \in G$ with $x = g \cdot y$. We prove this by double inclusion.

Let $h \in \mathrm{Stab}_G(x)$, we want to show that $h \in g\,\mathrm{Stab}_G(y)g^{-1}$.

Since $h \in \mathrm{Stab}_G(x)$, $h \cdot x = x = g \cdot y$, so we have

$$h \cdot x = h \cdot (g \cdot y) = (hg) \cdot y = (g \cdot y) \implies (g^{-1}hg) \cdot y = y$$

and so $h \in g\,\mathrm{Stab}_G(y)g^{-1}$ hence $\mathrm{Stab}_G(x) \subseteq g\,\mathrm{Stab}_G(y)g^{-1}$.

Now, given $h' \in g\,\mathrm{Stab}_G(y)g^{-1}$, we aim to show that $h' \in \mathrm{Stab}_G(x)$.

We have that there exists some $h \in \mathrm{Stab}_G(y)$ such that $h' = ghg^{-1}$. To show that h' stabilises x, consider

$$h' \cdot x = (ghg^{-1}) \cdot x = (gh) \cdot (g^{-1} \cdot x) = (gh) \cdot y = g \cdot y = x$$

and so $h' \in \mathrm{Stab}_G(x)$ and $g\,\mathrm{Stab}_G(y)g^{-1} \subseteq \mathrm{Stab}_G(x)$. Hence $\mathrm{Stab}_G(x) = g\,\mathrm{Stab}_G(y)g^{-1}$, as required. □

All transitive G-sets look like sets of left cosets, G/H for a suitable H. What H? Given a transitive G-set say X, then the subgroup it corresponds to (the conjugacy class of subgroups really) is the conjugacy class of point stabilisers. Note that if you take two different points in X, the stabiliser of each point are conjugate. Two conjugate subgroups give isomorphic G-sets, and hence a bijection arises for transitive G-sets and conjugate classes of subgroups of G. This leads us to the following corollary and theorem where we prove these notions formally. This will become clearer after you read the following proofs.

Corollary 14.7 (Consequence of Orbit Stabiliser)

Let G be a group and let X be a transitive G-set. Then X is isomorphic to G/H, for some $H \leq G$.

Proof. Let $x \in X$. As X is transitive, $\operatorname{Orb}_G(x) = X$, and so by the Orbit Stabiliser theorem we have $X \cong G/\operatorname{Stab}_G(x)$, where $\operatorname{Stab}_G(x) = H \leq G$. □

Remark 14.8. In the above proof, we can take $H = \operatorname{Stab}_G(x)$ for any $x \in X$. This makes sense since by Theorem 14.6 we have that any two point stabilisers are conjugate, and by Theorem 13.17, for any $x' \in X$, $G/\operatorname{Stab}_G(x) \cong G/\operatorname{Stab}_G(x')$.

In general, even if a G-set X is transitive, its points may have different stabilisers. In fact, stabilisers of different points in X will be the same if and only if the subgroup $\operatorname{Stab}_G(x)$ is normal in G. This can easily be shown.

Corollary 14.9

Let X be a transitive G-set and let $x \in X$. Then $\operatorname{Stab}_G(x)$ is normal in G if and only if $\operatorname{Stab}_G(x) = \operatorname{Stab}_G(y)$ for all $y \in X$.

Proof. First, assume that $\operatorname{Stab}_G(x)$ is normal in G, and let $y \in X$. By Theorem 14.6, there exists $g \in G$ such that $\operatorname{Stab}_G(y) = g\operatorname{Stab}_G(x)g^{-1}$, and since $\operatorname{Stab}_G(x)$ is closed under conjugation, $\operatorname{Stab}_G(y) = \operatorname{Stab}_G(x)$, as required.

Now assume that $\operatorname{Stab}_G(x) = \operatorname{Stab}_G(y)$ for all $x, y \in X$. Let $h \in \operatorname{Stab}_G(x)$. Then $h \cdot x = x$, and since X is transitive there exists $g \in G$ such that $x = g \cdot y$. We then have

$$h \cdot g \cdot y = g \cdot y \implies g^{-1}hg \cdot y = y,$$

so $g^{-1}hg \in \operatorname{Stab}_G(y) = \operatorname{Stab}_G(x)$, or equivalently $h \in g\operatorname{Stab}_G(x)g^{-1}$. So we have $\operatorname{Stab}_G(x) \subseteq g\operatorname{Stab}_G(x)g^{-1}$. Since y and therefore g is arbitrary, the previous statement is true for all $g \in G$, so $\operatorname{Stab}_G(x)$ is normal in G. □

Theorem 14.10

Let G be a group. Then there is a bijection between conjugacy classes of subgroups of G and isomorphism classes of transitive G-sets.

Proof. Let $\mathcal{C}$ denote the set of conjugacy classes of subgroups of G and $\mathcal{I}$ denote the set of isomorphism classes of transitive G-Sets. Define the map $\varphi : \mathcal{C} \to \mathcal{I}$ by sending the conjugacy class of a subgroup H to the isomorphism class of the transitive G-set G/H. Specifically, for a subgroup $H \leq G$, $\varphi([H]) = [G/H]$.

Conversely, define the map $\psi : \mathcal{I} \to \mathcal{C}$ by sending the isomorphism class of a transitive G-set X to the conjugacy class of the stabiliser of any point $x \in X$. That is, for a transitive G-set X, $\psi([X]) = [\operatorname{Stab}_G(x)]$.

Note that these maps are well defined by Theorem 13.17 and 14.6 respectively.

To show that φ and ψ are inverses, we prove that $\varphi \circ \psi = \mathrm{id}_{\mathcal{I}}$ and $\psi \circ \varphi = \mathrm{id}_{\mathcal{C}}$:

For $\varphi \circ \psi = \mathrm{id}_{\mathcal{I}}$, let $[X] \in \mathcal{I}$. Then $\psi([X]) = [\operatorname{Stab}_G(x)]$ for some $x \in X$. Applying φ, we get $\varphi(\psi([X])) = \varphi([\operatorname{Stab}_G(x)]) = [G/\operatorname{Stab}_G(x)]$. Since X is isomorphic to $G/\operatorname{Stab}_G(x)$ by the Orbit-Stabiliser Theorem, we have $\varphi(\psi([X])) = [X]$, proving that $\varphi \circ \psi$ is the identity on $\mathcal{I}$.

For $\psi \circ \varphi = \mathrm{id}_{\mathcal{C}}$, let $[H] \in \mathcal{C}$. Applying φ, we get $\varphi([H]) = [G/H]$. Then applying ψ, we have $\psi(\varphi([H])) = \psi([G/H]) = [\mathrm{Stab}_G(H)]$. By definition, the stabiliser of H in G/H is H itself, so $\psi(\varphi([H])) = [H]$, showing that $\psi \circ \varphi$ is the identity on $\mathcal{C}$.

Therefore, φ and ψ are inverse bijections, establishing the claimed correspondence. □

§15 Lecture 15

§15.1 Applications of Orbit-Stabiliser Theorem and Cauchy's Theorem

Definition 15.1. Let X be a G-set. We write $X^G := \{x \in X \mid \forall g \in G, g \cdot x = x\}$ to denote the set of fixed points of the action. In other words, X^G consists of all x in X with $\mathrm{Orb}_G(x) = \{x\}$. In particular, if X is finite then we have

$$|X| = \left|X^G\right| + \sum_{i=1}^{r} |\mathrm{Orb}_G(x_i)|,$$

where the sum runs over those orbits whose size are greater than one. This formula is called the class equation of the group action.

Lemma 15.2

Let G be a group of order p^n for some prime p and $n \geq 1$. If G acts on a finite set X, then

$$\left|X^G\right| \equiv |X| \bmod p.$$

Proof. Since G is a finite group, by the orbit-stabiliser theorem $|\mathrm{Orb}_G(x)|$ divides $|G| = p^n$ for all x. In particular, if $\mathrm{Orb}_G(x_i)$ is an orbit with $|\mathrm{Orb}_G(x_i)| > 1$ then we must have $|\mathrm{Orb}_G(x_i)| = p^k$ for some $1 \leq k \leq n$. Hence the result follows from considering the class equation of the group action (15.1):

$$|X| - \left|X^G\right| = \underbrace{\sum_{i=1}^{r} |\mathrm{Orb}(x_i)|}_{\text{multiple of } p} \implies \left|X^G\right| \equiv |X| \bmod p.$$

□

Theorem 15.3 (Cauchy's Theorem)

Let G be a finite group and p be a prime divisor of $|G|$. Then G contains an element of order p.

Proof. Consider the set

$$X = \{(x_1, \ldots, x_p) \in G^p \mid x_1 \cdots x_p = 1\}$$

of p-tuples of elements x_i of G whose product is the identity. Notice that such a p-tuple is uniquely determined by $p-1$ of its components. Indeed, if $x_1, \ldots, x_{p-1}$ is an arbitrary collection of elements in G then x_p is forced to be $x_p = (x_1 \cdots x_{p-1})^{-1}$. Thus, we see that X has $|G|^{p-1}$ elements and hence $|X|$ is divisible by p (as p is a divisor of $|G|$).

Now observe that the cyclic group $\mathbb{Z}_p = \langle\sigma\rangle$, for $\sigma = (123\cdots p) \in S_p$, acts on X by

$$\sigma \cdot (x_1, \ldots, x_p) = \big(x_{\sigma(1)}, \ldots, x_{\sigma(p)}\big) = (x_2, \ldots, x_p, x_1)$$

The RHS does indeed remain in X since $x_1 \cdots x_p = 1$ implies $x_1^{-1} = x_2 \cdots x_p$ and hence $x_2 \cdots x_p \cdot x_1 = 1$. Moreover, we can apply Lemma 15.2 to this action to conclude that $\left|X^{\mathbb{Z}_p}\right| \equiv 0 \bmod p$. The set of fixed points of this action is given by

$$X^{\mathbb{Z}_p} = \{(x, \ldots, x) \in G^p \mid x \cdots x = 1\}$$

since σ fixes $(x_1, \ldots, x_p)$ iff $x_1 = x_2 = \cdots = x_p$. This set is non-empty, since $(1, \ldots, 1) \in X^{\mathbb{Z}_p}$, and so $\left|X^{\mathbb{Z}_p}\right| \geq p$.

This implies that there exists an $x \in G$ with $x \neq 1$ such that $(x, \ldots, x) \in X^{\mathbb{Z}_p}$; that is, $x^p = 1$. □

Theorem 15.4

Let G be a finite group and p be the smallest prime dividing $|G|$. Let H be a subgroup of index p. Then H is normal in G.

Proof. Consider the action of H on the set of left cosets G/H. By the orbit-stabiliser theorem, the size of every orbit of cosets divides $|H|$, and hence also divides $|G|$. Since there are exactly p elements of G/H, any orbit must simultaneously divide $|G|$ and have cardinality at most p, so either we have a single orbit of size p or there are p different orbits of size 1, since p is the smallest prime divisor of $|G|$.

Clearly the first option is impossible, since $H \in G/H$ is a fixed point under the action; there is an orbit of size 1, so they must all be of size 1. This means that all of our cosets are fixed points, and for every $h \in H$, $g \in G$, we have $hg^{-1}H = g^{-1}H$. So, $\exists h' \in H$ s.t. $hg^{-1} = g^{-1}h'$, and hence $ghg^{-1} = h' \in H$, so H is normal in G. □

Remark 15.5. We are already familiar with this result for index 2 subgroups by Theorem 6.6. We should note that a subgroup of index p is not guaranteed to exist.

§16 Lecture 16

§16.1 Not Burnside's Lemma

Applications of Cauchy's Theorem and Burnside's lemma (not Burnside's work!)

Example 16.1 (Classify groups of order 6)

Let G be a group of order 6. Then G is either cyclic or isomorphic to $S_3 \equiv D_6$.

Proof. Let G be a group of order 6. By Cauchy's Theorem, there exists an element $h \in G$ of order 2 and an element $k \in G$ of order 3. Notice that $K = \langle k\rangle$ has index 2 by Lagrange, and so by Theorem 15.4 it must be normal in G. Also, considering orders we can see that $G = \{1_G, k, k^2, h, hk, hk^2\}$ since each of these elements must be distinct. In other words, $G = \langle h, k\rangle$.

Recall that an automorphism is an isomorphism from a group to itself. Since K is of prime order p, the set of automorphisms of K, $\mathrm{Aut}(K)$, must have size $p-1$ (proved in ex sheet 2 Q11), so $|\mathrm{Aut}(K)| = 2$; note that we have actually seen this directly using multiplication tables in Example 3.4. Let $\varphi \in \mathrm{Aut}(K)$ be the identity map $k \mapsto k$ and $\psi \in \mathrm{Aut}(K)$ be the map defined by $k \mapsto k^2$.

Furthermore, we claim that

$$\begin{aligned} \phi_K : K &\to K \\ \tilde{k} &\mapsto h\tilde{k}h^{-1} \end{aligned}$$

is an automorphism of K, i.e. a bijective homomorphism.

Since K is normal in G, we have $h\tilde{k}h^{-1} \in K$ for $\tilde{k} \in K$, so K is indeed the codomain. Furthermore, for any two $k_1, k_2 \in K$, we have

$$\phi_K(k_1k_2) = h(k_1k_2)h^{-1} = hk_1(h^{-1}h)k_2h^{-1} = \phi_K(k_1)\phi_K(k_2),$$

hence ϕ_K is a group homomorphism. Finally, because h has order 2,

$$\phi_K^2(\tilde{k}) = h(h\tilde{k}h^{-1})h^{-1} = h^2\tilde{k}h^{-2} = \tilde{k},$$

and so ϕ_K is self-inverse (bijective), so it is indeed an automorphism.

Now since $\phi_K \in \mathrm{Aut}(K) = \{\varphi, \psi\}$, we have two cases to check.

First, suppose $\phi_K = \varphi$, i.e. $hkh^{-1} = k$. Then $hk = kh$, and so h and k commute. Imposing this condition, we can see that the element $hk \in G$ has order 6, since $(hk)^n = h^nk^n$, and so $|hk| = \mathrm{lcm}(|h|, |k|) = 6$. Therefore hk is a generator for G, and hence G is cyclic.

On the other hand, suppose $\phi_K = \psi$, i.e. $hkh^{-1} = k^2 = k^{-1}$. Then

$$G = \langle h, k \mid h^2 = k^3 = 1_G, hk = k^{-1}h \rangle \cong D_6 \cong S_3.$$

□

Definition 16.2. Let G be a group, $g \in G$ and X the associated G-Set. Then we denote $X^g := \{x \in X \mid g \cdot x = x\}$, that is, all the points in X that are fixed by a specific element $g \in G$.

> **Remark 16.3.** Do not confuse this with X^G, the set of fixed points of an action.

Definition 16.4. Let G be a group and X be a G-set. The set of G-orbits of X is denoted by X/G. Thus we have $X = \bigsqcup_{\mathcal{O} \in X/G} \mathcal{O}$.

> **Remark 16.5.** Note that the above definition uses disjoint union.

Theorem 16.6 (Not Burnside's Lemma)

Let G be a group and X be a G-set. We have

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof. Consider the set $S = \{(g, x) \in G \times X \mid g \cdot x = x\}$. We will show the required equality by counting S in two different ways. On the one side, for each element $g \in G$, we can count the number of elements $x \in X$ satisfying $g \cdot x = x$; this is exactly $|X^g|$ by definition. But in the definition of S we are free to choose $g \in G$, so $|S| = \sum_{g \in G} |X^g|$.

On the other hand, we can count the $g \in G$ for each $x \in X$ such that $g \cdot x = x$. Notice that this is just $|\operatorname{Stab}_G(x)|$, which is $|G|/|\operatorname{Orb}_G(x)|$ by the Orbit-Stabiliser Theorem. Let $\mathcal{O} = \operatorname{Orb}_G(x)$ for this section only. Then,

$$|S| = \sum_{x \in X} |\operatorname{Stab}_G(x)| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}|}.$$

We can translate this sum over all elements of X to a sum over all elements of each orbit:

$$|S| = |G| \sum_{\mathcal{O} \in X/G} \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} = |G| \sum_{\mathcal{O} \in X/G} 1 = |G||X/G|.$$

Hence

$$|G||X/G| = \sum_{g \in G} |X^g|,$$

as required. □

Recall that an orbit of a G-set is a collection of elements that can be transformed into each other by the group action. In other words, it is a set of points that become indistinguishable under the symmetries of the set under the group action. This is important as it allows us to count each distinct arrangement only once, omitting any symmetrical equivalents.

Remark 16.7. An important application of group actions and orbit counting is simplifying counting problems. The next example demonstrates this by counting the distinct ways to color a triangle, considering its symmetries.

Example 16.8

How many essentially different ways are there of coloring the sides of a triangle using four colours? Essentially different in that one coloring cannot be obtained from the other by applying symmetries of the triangle.

Proof. This can be done using non-Burnside's Lemma. Let X be the set of all genuinely different colourings for the triangle sitting still. Then $|X| = 4^3 = 64$ as we have four colours to choose from for each side. Consider the group D_6 acting on X. Two colourings are essentially different if one cannot be obtained from the other by applying symmetries of the triangle, i.e. if they lie in different orbits under the action of D_6. So the number of essentially different colourings is just the number of orbits, $|X/G|$, which is given by

$$|X/G| = \frac{1}{|G|} \sum_{\sigma \in D_6} |X^\sigma|.$$

We will now count $|X^\sigma|$ for each $\sigma \in D_6$. In other words, we are counting the number of triangle colourings that are fixed by each $\sigma \in D_6$.

First consider $\sigma = e$. The identity fixes all $x \in X$, so $|X^e| = |X| = 64$.

Next, consider σ a reflection through an axis of symmetry. For the triangle to be fixed, we require the two faces we're swapping to be the same colour. We therefore have 4 choices in the first face, then the opposite w.r.t. the axis of symmetry is decided (no choice), and we have 4 choices for the third face. Hence $|X^\sigma| = 16$. Note that we have three such $\sigma \in D_6$ corresponding to each axis of symmetry so we count $3 \cdot 16 = 48$.

Finally, consider σ a (single) rotation. For the triangle to stay the same, we require all 3 sides to be the same; we have one choice from four colors. Therefore, $|X^\sigma| = 4$. We have 2 different rotations (the third rotation in the triangle is just the identity), so we count $2 \cdot 4 = 8$.

Then, by Burnside's,

$$|X/G| = \frac{1}{6}(64 + 8 + 48) = 20.$$

□

§17 Lecture 17

- (Non-Examinable)

§17.1 Semi-direct product

We will now introduce the semi-direct product, which is a generalisation of the direct product. Recall from Definition 10.3 that the direct product is the group theory analogue to the cartesian product in set theory. For example, we can make groups like $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Consider a group G with subgroups H and N, and let $H \cap N = \{e\}$ and $NH = G$. Now consider the map

$$\begin{aligned} \phi : N \times H &\to G \\ (n, h) &\mapsto nh. \end{aligned}$$

Assume we have $h_1, h_2 \in H$ and $n_1, n_2 \in N$ such that $n_1 h_1 = n_2 h_2$. We then have $n_2^{-1} n_1 = h_2 h_1^{-1} = e$ since $H \cap N = \{e\}$. This shows that ϕ is injective.

Now, consider $\operatorname{Im} \phi = \{nh : h \in H, n \in N\} = NH = G$, so ϕ is surjective.

Therefore, when considering $N \times H$ and G as sets, they are in bijection.

What if we would like ϕ to be a group isomorphism? In other words, what if we would like to reconstruct G from the subgroups H and N? We need to find a group law, a way to multiply the elements of $N \times H$ together, that gives

$$\phi((n_1, h_1)(n_2, h_2)) = \phi((n_1, h_1))\phi((n_2, h_2)) = n_1 h_1 n_2 h_2.$$

We can write,

$$n_1 h_1 n_2 h_2 = n_1 h_1 n_2 h_1^{-1} h_1 h_2.$$

We therefore need

$$\phi((n_1, h_1)(n_2, h_2)) = n_1 h_1 n_2 h_1^{-1} h_1 h_2 = \phi(n_1 h_1 n_2 h_1^{-1}, h_1 h_2).$$

We have $h_1 h_2 \in H$. If we assume in addition that N is normal in G, then N is closed under conjugation by elements of G, and therefore $n_1 h_1 n_2 h_1^{-1} \in N$.

As ϕ is an injection, we need

$$(n_1, h_1)(n_2, h_2) = (n_1 h_1 n_2 h_1^{-1}, h_1 h_2).$$

If we define the group multiplication of $N \times H$ as above, we have that ϕ is also a group homomorphism.

We can represent this multiplication in another way. For each $h \in H$, let φ_h be a group automorphism of N defined by conjugation by the element h. We can construct a group homomorphism,

$$\begin{aligned} \varphi : H &\to \mathrm{Aut}(N) \\ h &\mapsto \varphi_h. \end{aligned}$$

We can then rewrite the group multiplication as

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2).$$

You can check that the set $N \times H$ with the above multiplication does indeed form a group. This group is denoted $N \rtimes_\varphi H$.

Definition 17.1. Let G be a group and let $H \leq G$, $N \trianglelefteq G$ such that $H \cap N = \{e\}$ and $HN = G$. Then G is called an *(internal) semi-direct product* of H and N.

Now consider groups N and H that can now be completely separate groups. What if we would like to create a new group out of them, say G, such that N and H satisfy similar conditions to that of an internal semi-direct product. Since N and H can be completely separate, we will define $N_G \cong N$ and $H_G \cong H$ such that these are subgroups of G. In other words, we want to find a group G such that $N_G \trianglelefteq G$, $H_G \leq G$, $N_G \cap H_G = \{e_G\}$, and $N_G H_G = G$.

Consider $G = N \times H$, $N_G = N \times \{e_H\}$, and $H_G = \{e_N\} \times H$. We can check that our original conditions are satisfied: $N_G \cap H_G = \{(e_N, e_H)\}$ and $N_G H_G = G$ using set builder.

Now let us consider the multiplication of two arbitrary elements of G. Let (n_1, h_1), $(n_2, h_2) \in G$. We have,

$$\begin{aligned} (n_1, h_1)(n_2, h_2) &= (n_1, e_H)(e_N, h_1)(n_2, e_H)(e_N, h_2) \\ &= (n_1, e_H) \underbrace{(e_N, h_1)(n_2, e_H)(e_N, h_1^{-1})}_{(n, e_H)} (e_N, h_1)(e_N, h_2) \end{aligned}$$

where we require $(e_N, h_1)(n_2, e_H)(e_N, h_1^{-1}) = (n, e_H)$ for $n \in N_G$ as we need closure under conjugation for $N_G \trianglelefteq G$.

For this to work, we need a group homomorphism $\phi : H \to \mathrm{Aut}(N)$, defined by $h \mapsto \phi_h \in \mathrm{Aut}(N)$, so that we can define the group multiplication as

$$(n_1, h_1)(n_2, h_2) = (n_1 \phi_{h1}(n_2), h_1 h_2),$$

meeting the condition of $N_G \trianglelefteq G$.

Definition 17.2. Given groups N and H, and a group homomorphism $\phi : H \to \mathrm{Aut}\, N$ we define the *(external) semidirect product* of N and H (wrt ϕ), written $N \rtimes H$ or $N \rtimes_\phi H$, with the multiplication operation,

$$(n, h)(n', h') = (n \phi_h(n'), hh').$$

Remark 17.3. Notice that in the definition of the internal semi-direct product, we are starting with a subgroup H and a normal subgroup N in G, and reconstructing G by combining the elements of H and N in a specific way that reflects the internal structure and symmetries of G.

Meanwhile, in the external semi-direct product, we take groups N and H, which can be completely unrelated, and form a new group G out of them.

Also note that for an external semi-direct product of N and H, the groups N_G and H_G as defined earlier form an internal semi-direct product G.

Remark 17.4. If in the definition of the semi direct product we take $\phi : H \to \operatorname{Aut} N$ to be the trivial homomorphism, then we recover the definition of the direct product.

Example 17.5

For $n \in \mathbb{Z}_{\geq 3}$, the dihedral group D_{2n} is a semidirect product of the normal subgroup $\langle \sigma \rangle$ and the subgroup $\langle \tau \rangle$, where $\sigma^n = \tau^2 = e$. Here, $\phi : \langle \tau \rangle \to \operatorname{Aut}\langle \sigma \rangle$ sends τ to the inversion automorphism, $\phi_\tau : \sigma^i \mapsto \sigma^{-i}$.

Theorem 17.6

Every group of order 15 is cyclic.

Proof. Let G be a group of order 15. By Cauchy's Theorem, we have $g, h \in G$ where g is an element of order 5 and h of order 3. Moreover, $\langle g \rangle$ has order 5, and therefore has index 3 by Lagrange. Since 3 is the smallest prime divisor of $|G|$, by Theorem 15.4 it follows that $N = \langle g \rangle \trianglelefteq G$.

Let $H = \langle h \rangle$, then $H \cap N$ is a normal subgroup of H by the second isomorphism theorem, and by Lagrange, it follows that $|H \cap N|$ must divide 3, i.e. $|H \cap N|$ is either 3 or 1. Furthermore, $H \cap N$ is a subgroup of N. Hence, its order must also divide 5 or 1, so $H \cap N = \{1\}$. Therefore, $NH = G$.

We have therefore shown that $G = N \rtimes H$. Hence, conjugation by H defines a group homomorphism $\phi : H \to \operatorname{Aut} N$, but $|\operatorname{Aut} N| = 4$. Moreover, $\operatorname{Im}\phi \leq \operatorname{Aut} N$, hence $|\operatorname{Im}\phi|$ divides $|\operatorname{Aut} N| = 4$, but by FIT and Lagrange, $|\operatorname{Im}\phi|$ also divides $|H| = 3$, hence $|\operatorname{Im}\phi| = 1$, i.e. the image of ϕ is trivial. Therefore every element of H gives rise to the trivial automorphism of N, and since conjugating by every element of h leaves $n \in N$ unchanged, h and n commute.

Hence, $G = N \times H$. Since N is cyclic of order 5 and H is cyclic of order 3, from ex sheet 2 Q10, $G \cong N \times H$. Therefore, G is cyclic and $G = \langle n \cdot h \rangle$. □

§18 Lecture 18

§18.1 Intro to rings

Definition 18.1. A ring is a collection $(R, +, \cdot)$ where R is a set, and $+$ and $\cdot$ are two binary operations on R such that

(R1): $(R, +)$ is an abelian group (call the additive identity 0);

(R2): The operation $\cdot$ is associative, i.e. for any $a, b, c \in R$ one has

$$(a \cdot b) \cdot c = a \cdot (b \cdot c);$$

(R3): $\cdot$ distributes over $+$, i.e. for all $a, b, c \in R$ one has

$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ and } c \cdot (a + b) = c \cdot a + c \cdot b.$$

A *unital ring* or a *ring with unity* is a ring as above such that there exists $1 \in R \setminus \{0\}$ satisfying $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. A ring is called *commutative* if the operation $\cdot$ is commutative.

Remark 18.2. Note that many authors will refer to a unital ring simply as a ring, and will call a ring without a unit a *rng*.

Example 18.3

We have already seen examples of rings such as $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. The following are some more interesting examples.

- For every $n \in \mathbb{Z}_{>1}$, the set of cosets $\mathbb{Z}/n\mathbb{Z}$ forms a ring under addition and multiplication modulo n.
- If R is a commutative ring, then one can form the ring $R[X]$ of polynomials over R in one variable. These polynomials are expressed as formal sums of the form $\sum_{i=0}^{d} a_i X^i$, where $d \in \mathbb{Z}_{\geq 0}$, $a_i \in R$ for all i, and the addition and multiplication are defined as the usual addition and multiplication for polynomials..
- if R is a ring, then one can form the ring $M_n(R)$ of $n \times n$ matrices over R under matrix addition and multiplication.
- If R is a ring and S is an arbitrary set, the set R^S of functions $f : S \to R$ is a ring under pointwise addition and multiplication: $(f+g)(s) = f(s)+g(s), (f \cdot g)(s) = f(s) \cdot g(s)$.

  If $S = \mathbb{N}$ then the function f assigns every natural number some element of R, i.e. elements of R^S are sequences of elements of R, and we can add and multiply pointwise elements of the sequence.
- The most boring ring is the trivial ring, containing a single element. This is indeed commutative and unital, and the only ring in which 0 and 1 coincide.

Remark 18.4. Let R be a ring, and $a, b \in R$, $n \in \mathbb{Z} \setminus \{0\}$. We use the following conventions and notation.

1. The notation $n \cdot a$ is shorthand for

$$\underbrace{a + a + \cdots + a}_{n \text{ times}}$$

in the ring. Similarly, premultiplication by a negative integer denotes repeated addition of the additive inverse of a. In other words, if $n \in \mathbb{Z}_{<0}$, then $n \cdot a$ represents

$$\underbrace{-a - a - \cdots - a}_{|n| \text{ times}}.$$

2. Write $a - b = a + (-b)$.
3. If R is unital, we set $a^0 = 1$ for any $a \in R \setminus \{0\}$. Note however that a^{-1} won't exist in general.
4. We usually drop $\cdot$ and instead write ab rather than $a \cdot b$.

Theorem 18.5

Let R be a ring, let $a, b \in R$, and let $m, n \in \mathbb{Z}$. Then we have

1. $0a = a0 = 0$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $(m + n) \cdot a = m \cdot a + n \cdot a$;
5. $(mn) \cdot a = m \cdot (n \cdot a)$;
6. $m \cdot (a + b) = m \cdot a + m \cdot b$;
7. $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$;
8. $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$.

Proof. Exercise. □

Remark 18.6. Note that in rings, ab do not need to commute, the multiplicative identity may not exist, and the cancellation rule does not need to hold. Be careful with these intuitive ideas; try to derive everything directly from the axioms.

Also, note that item 4 above is not the distributivity rule from the axioms as m and n are integers and not ring elements.

Definition 18.7. Let R be a unital ring. An element u of R is called a *unit* if there exists $u^{-1} \in R$ such that $uu^{-1} = u^{-1}u = 1$. The set of units of R is denoted by $R^\times$ and forms a group under the multiplication operation in R.

Definition 18.8. A unital ring in which every non-zero element is a unit is called a *division ring*. A commutative division ring is called a *field*.

Example 18.9

The Hamilton quaternions $\mathbb{H}$ are a real vector space with basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$, with multiplication defined by

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = 1, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$$

and extended to $\mathbb{R}$-linear combinations by distributivity. The inverse of an arbitrary element $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \neq 0$ is

$$\frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

This is a division ring but not a field. The non-commutativity of the multiplication is the only property that keeps the quaternions from being a field.

§19 Lecture 19

§19.1 Subrings, ideals, and quotients

Definition 19.1. Let R be a ring. A *subring* of R is an additive subgroup $S \subset R$ s.t. for every $a,\ b \in S$, one has $ab \in S$. We usually write $S \leq R$ to say that S is a subring of R. If R is unital, a subring $S \leq R$ is called a unital subring if $1 \in S$.

Remark 19.2. Note that although we mainly consider unital subrings, a subring of a unital ring need not be unital. For example, $2\mathbb{Z} \leq \mathbb{Z}$ does not contain 1.

Example 19.3

We have the chain of subrings $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{H}$. Here are some more interesting examples.

- If R is a commutative ring, then R itself is a subring of the ring of polynomials $R[X]$.
- Let S be a subring of the (unital) ring R. Then for every $n \in \mathbb{Z}_{>0}$ we have $M_n(S)$ is a subring of the (unital) ring $M_n(R)$.
- Consider the set of all functions $f : \mathbb{N} \to \mathbb{R}$, i.e. all sequences of real numbers. Define addition and multiplication pointwise with elements of the sequence. The sequence of zeroes is the additive identity, and the subset of all sequences that converge to 0 is a subring. This subring is not unital, since the multiplicative identity would have to be the sequence of ones, which does not converge to 0.

We will now move our attention to forming quotient rings. Recall that normal subgroups form quotient groups. What substructures do we need to consider to form quotient rings? That depends on the kind of quotient structure we aim for: additive $(r + S)$ or multiplicative cosets (rS)?

We can look at existing cosets, namely $\mathbb{Z}/n\mathbb{Z}$. We will try to build cosets whose elements consist of additive cosets.

Note that as a group, rings are abelian, so every subring will also be an abelian subgroup.

We know then that the operation for additive cosets of rings is well defined as all subgroups of an abelian group are normal. We now need a condition to ensure the well definedness of multiplication of cosets for rings.

Let $I \subset R$ be an additive subgroup, and let $a,\ b \in R$. We want to define multiplication of cosets as $(r+I)(s+I) = (rs)+I$. So when is this well defined?

Let $r+I = r'+I$ and $s+I = s'+I$. This gives that there exists some $i, j \in I$ such that $r' = r+i$ and $s' = s+j$. We need $r's'+I = rs+I$ for the operation to be well defined. Consider

$$r's' - rs = (r+i)(s+j) - rs = rj + is + ij.$$

As $r's' - rs \in I \implies r's'+I = rs+I$, we need to ensure $rj + is + ij \in I$.

We have now motivated our definition for an ideal; we want that for every $i \in I$ and $r \in R$ one has $ri, ir \in I$. We can split this into 3 types of ideals: left, right and two-sided.

> **Remark 19.4.** Spoiler alert: The two-sided ideals are exactly the conditions we need to create well-defined multiplication of cosets.

Definition 19.5. Let R be a ring. A *left ideal* of R is an additive subgroup I of R s.t. for every $a \in I$ and $r \in R$, $ra \in I$. That is, for every $r \in R$, we have $rI \subseteq I$.

A *right ideal* of R is an additive subgroup I of R s.t. for every $a \in I$ and $r \in R$, $ar \in I$. That is, for every $r \in R$, we have $rI \subseteq I$.

A *two-sided ideal* is an additive subgroup I of R that is a left ideal and a right ideal. We write $I \trianglelefteq R$ and say I is an ideal of R.

An ideal of R is called *proper* if it is not equal to R.

> **Remark 19.6.** If a two-sided ideal I of R contains 1, then $I = R$, since by properties of ideals, $1r = r \in I$, $\forall r \in R$. This means that no proper ideal can be a unital subring.

> **Remark 19.7.** In any ring R, the trivial and maximal subrings $\{0_R\}$ and R are ideals. In a field F, if a non-zero element $x \in F$ is present in an ideal, then so is $xx^{-1} = 1$. This means that these are the only ideals in a field.

Definition 19.8. Let R be a unital ring, and I be a proper two-sided ideal in R. The *quotient ring* R/I has, as its underlying set, the set of cosets $\{r+I \mid r \in R\}$. We define the addition of cosets as $(r+I)+(s+I) = (r+s)+I$ and multiplication as $(r+I)(s+I) = (rs)+I$.

Note that we have an equivalent condition as with group cosets for two elements of R/I having different representatives but being the same coset. We have $r+I = s+I \iff r-s \in I$.

Example 19.9

Let $R = \mathbb{R}[X]$, and consider the subset $I = X^2R = \{a_2X^2 + a_3X^3 + \cdots a_dX^d \in \mathbb{R}[X] : d \in \mathbb{Z}_{\geq 2},\ a_i \in \mathbb{R}\}$. We can check that this is an additive subgroup of R. Now let $r \in R$ and $i \in I$. As i has degree at least 2, the product ri will also have degree at least 2, so $ri = ir \in I$. Therefore X^2R is an ideal of R.

Let us now consider the quotient ring R/I. Two polynomials $f = a_0 + a_1x + \cdots$, $g = b_0 + b_1x + \cdots \in R$ represent the same coset in R/I if and only if $a_0 = b_0$, $a_1 = b_1$, so that $f - g \in I$. In other words, for each $a, b \in \mathbb{R}$, the coset $a + bx + I$ is unique. Thus, R/I can be thought of as a plane where each point, or coset, is uniquely determined by a linear polynomial $a + bX + I$. Therefore, R/I can be can be seen as a 2-dimensional vector space spanned by $\hat{1} = 1 + I$, $\hat{X} = X + I$, with the property that $\hat{X}^2 = 0$, since $X^2 + I = 0 + I = I$.

§20 Lecture 20

§20.1 Ring homomorphisms

Example 20.1

Let $R = \mathbb{R}[X]$ and consider the subring $I = (X^2 + 1)R$, which is a two-sided ideal. It can be shown that every coset $f + I$ contains a unique polynomial of the form $a_0 + a_1x$. It follows that R/I is a 2-dimensional vector space $\mathbb{R}$ spanned by $\hat{1} = 1 + I$, $\hat{X} = X + I$. We have the additional property that $\hat{X}^2 = -\hat{1}$, since $\hat{X}^2 = X^2 + I = (X^2 + 1) + I - (1 + I)$.

Definition 20.2. Let R, S be rings. A *ring homomorphism* from R to S is a function $\phi : R \to S$ such that for all a, $b \in R$ we have

1. $\phi(a + b) = \phi(a) + \phi(b)$;
2. $\phi(ab) = \phi(a)\phi(b)$.

If R and S are unital, then a ring homomorphism is called *unital* if $\phi(1_R) = 1_S$. Unless otherwise stated, a homomorphism between unital rings will be assumed to be unital.

Remark 20.3. A ring homomorphism is a homomorphism of additive groups. It is not necessarily a homomorphism of multiplicative groups (as rings are not groups under multiplication in general), but it must still respect the operation.

Definition 20.4. We say that a ring homomorphism is an *isomorphism* if it has a two-sided inverse $\phi^{-1} : S \to R$, also a ring homomorphism. Symbolically, we have

$$\phi \circ \phi^{-1} = \mathrm{id}_S \quad \phi^{-1} \circ \phi = \mathrm{id}_R.$$

Theorem 20.5

A ring homomorphism is an isomorphism if and only if it is bijective.

Proof. Clearly any isomorphism must be bijective, so there is nothing to check in the

forward direction — we must only check that a bijective ring homomorphism is necessarily an isomorphism.

($\Longleftarrow$) We have that if $\phi : R \to S$ is a bijective ring homomorphism then ϕ^{-1} is also a group homomorphism of addition; it remains to check multiplication is preserved.

We claim that ϕ^{-1} also preserves multiplication, i.e. $\forall g, h \in S$,

$$\phi^{-1}(gh) = \phi^{-1}(g)\phi^{-1}(h).$$

If $g, h \in S$, then by the surjectivity of ϕ we have $x, y \in R$ such that $g = \phi(x)$ and $h = \phi(y)$. Then

$$\phi^{-1}(gh) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(g)\phi^{-1}(h),$$

as required. □

Example 20.6

Let R be a unital ring and I be a proper two-sided ideal. The quotient map $R \to R/I$, $r \mapsto r + I$ is a ring homomorphism.

Recall that for $I = (X^2+1)\mathbb{R}[X]$, we had the property that $\hat{X}^2 = -\hat{1}$, hence it might not be surprising that $\mathbb{R}[X]/I \to \mathbb{C}$ sending $\hat{X}$ to $i \in \mathbb{C}$ is a ring isomorphism.

Definition 20.7. Let $R \leq S$ be rings and $s \in S$. Then the *evaluation map* at s is defined by

$$\begin{aligned} \phi_s : R[X] &\to S \\ f &\mapsto f(s). \end{aligned}$$

If $f = a_0 + a_1X + \cdots + a_dX^d$, then we say $f(s) = a_0 + a_1s + \cdots + a_ds^d$.

Remark 20.8. If R is commutative, then the evaluation map is a ring homomorphism. We will see that this is a common way to induce ring isomorphisms.

§21 Lecture 21

§21.1 Isomorphism of rings and cancellation

Recall that a subring $U \subset R$ is an additive subgroup of R such that for all $r, r' \in U$ we have $rr' \in U$.

Definition 21.1. Let $\phi : R \to S$ be a ring homomorphism. The *kernel* of ϕ is defined as $\ker \phi = \{r \in R \mid \phi(r) = 0_S\}$ and the *image* of ϕ is defined as $\operatorname{Im} \phi = \{\phi(r) \mid r \in R\} \subseteq S$.

Theorem 21.2 (First Isomorphism Theorem for Rings)

Let $\phi : R \to S$ be a ring homomorphism of unital rings. Then

1. The kernel $\ker \phi$ is a proper ideal of R;
2. The image $\operatorname{Im} \phi$ is a subring of S;
3. The mapping

$$\begin{aligned} \psi : R/\ker \phi &\to \operatorname{Im} \phi \\ r + \ker \phi &\mapsto \phi(r) \end{aligned}$$

is a well-defined isomorphism.

Proof. (1) Note that $\ker \phi$ is an additive subgroup by FIT of groups. Moreover, note that for $k \in \ker \phi$ and $r \in R$ we have $\phi(rk) = \phi(r)\phi(k) = \phi(r)0 = 0$ so $rk \in \ker \phi$ and similarly $kr \in \ker \phi$. Also note that $1 \notin \ker \phi$ since we have that $\phi(1_R) = 1_S \neq 0_S$. Hence $\ker \phi \lhd R$.

(2) Note that $\operatorname{Im} \phi$ is an additive subgroup by FIT of groups. Moreover, let $s, s' \in \operatorname{Im} \phi$, so $\exists r, r' \in R$ s.t. $\phi(r) = s, \phi(r') = s'$. Since ϕ is a ring homomorphism,

$$\phi(rr') = \phi(r)\phi(r') = ss',$$

so $ss' \in \operatorname{Im} \phi$.

(3) By FIT for groups, we have that the isomorphism exists for the additive group structure with $\psi : R \to \operatorname{Im} \phi$ defined by $\psi(r + \ker \phi) = \phi(r)$. As ψ is bijective, we are left to show that ψ preserves multiplication. Let $r_1, r_2 \in R$. Then

$$\begin{aligned} \psi(r_1 + \ker \phi)\psi(r_2 + \ker \phi) &= \phi(r_1)\phi(r_2) \\ &= \phi(r_1 r_2) \\ &= \psi(r_1 r_2 + \ker \phi) \\ &= \psi((r_1 + \ker \phi)(r_2 + \ker \phi)). \end{aligned}$$

Therefore, we have a bijective ring homomorphism, hence the claim follows. □

Example 21.3 (In algebraic number theory)

Consider the homomorphism $\phi : \mathbb{R}[X] \to \mathbb{C}$, $f \mapsto f(i)$. This is a surjective ring homomorphism onto $\mathbb{C}$. Furthermore, $\ker \phi$ is the ideal generated by $X^2 + 1$, since this is the set of all real polynomials with i as a root. Hence by the FIT, $\mathbb{R}[X]/(x^2 + 1)\mathbb{R}[X] \cong \mathbb{C}$.

Note that as a vector space over $\mathbb{R}$, $\mathbb{C}$ is 2-dimensional, while $\mathbb{R}[X]$ is infinitely dimensional. Hence we just need two elements of $\mathbb{R}$ to represent every coset. This should make sense, as we often express an arbitrary complex number z as $a + ib$, where $a, b \in \mathbb{R}$.

Example 21.4 (In analysis)

Consider the set of continuous functions on $\mathbb{R}$, $C^0(\mathbb{R})$. This is a ring under pointwise addition and multiplication. The evaluation map

$$\begin{aligned} \phi : C^0(\mathbb{R}) &\to \mathbb{R} \\ f &\mapsto f(0) \end{aligned}$$

is a ring homomorphism, where the image is $\mathbb{R}$ and the kernel is

$$\ker \phi = \{f \in C^0(\mathbb{R}) \mid f(0) = 0\},$$

i.e. all the functions that pass through the origin. Hence $C^0(\mathbb{R})/\ker \phi \cong \mathbb{R}$.

Theorem 21.5

Let F be a field and R a non-trivial ring. Then every homomorphism $F \to R$ is injective.

Proof. Let $\phi : F \to R$ be a ring homomorphism. Assume that $\ker \phi$ is not trivial, and hence ϕ is not injective. Then there exists a non-zero element $f \in F$, s.t. $f \in \ker \phi$, i.e. $\phi(f) = 0_R$. Since F is a field, we have $f^{-1} \in F$ s.t. $f^{-1}f = 1_F$. So,

$$1_R = \phi(1_F) = \phi(ff^{-1}) = \phi(f)\phi(f^{-1}) = 0_R.$$

Hence R must be the trivial ring, a contradiction. □

Remark 21.6. Note that we did not use the fact that F is commutative. In fact, F does not need to be field, but just a division ring.

Definition 21.7. Let R be a ring. An element $a \in R$ is a *left zero divisor* if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ s.t. $ab = 0$. A right zero divisor is defined analogously.

Example 21.8

Consider $\mathbb{Z}/8\mathbb{Z}$. Then $2+8\mathbb{Z}$ is a zero divisor since it is non-zero and $(2+8\mathbb{Z})(4+8\mathbb{Z}) = 8 + 8\mathbb{Z} = 0 + 8\mathbb{Z}$.

Consider $R = \mathbb{R}[X]/X^2\mathbb{R}[X]$. The element $X + X^2\mathbb{R}[X]$ is a zero divisor since taking its square gives $0 + X^2\mathbb{R}[X]$.

Theorem 21.9

Let R be a ring. The following are equivalent

1. R has no left zero divisors;
2. R has no right zero divisors;
3. For all $a, b, c \in R$ with $a \neq 0$, one has $ab = ac$ if and only if $b = c$;
4. For all $a, b, c \in R$ with $a \neq 0$, one has $ba = ca$ if and only if $b = c$.

Proof. (1 $\iff$ 2) This is trivial by the definition of a zero divisor.

(2 $\implies$ 3) Suppose $ab = ac$ for some $a, b, c \in R$ with $a \neq 0$. We have $a(b-c) = 0$, and since R has no right zero divisors and $a \neq 0$, we must have $b - c = 0 \implies b = c$, as required.

(3 $\implies$ 2) Assume for contradiction that there is a right zero divisor in R. Then there exists $a, b \in R \setminus \{0\}$ with $ab = 0$. Now consider $c = 0 \in R$. We have $ac = a0 = 0 = ab$, and from (3) we have $b = c = 0$, a contradiction. So, R has no right zero divisors.

(1 $\implies$ 4) Shown by a symmetric argument to (2 $\implies$ 3).

(4 $\implies$ 1) Shown by a symmetric argument to (3 $\implies$ 2).

From above, we have (3) $\implies$ (2) $\implies$ (1) $\implies$ (4), and therefore we have the chain (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) $\implies$ (1), so all four statements are equivalent. □

Theorem 21.10

Let R be a unital ring and let $u \in R$ be a unit. Then u is is not a zero divisor.

Proof. Let u be a unit and assume there exists $v \in R$ s.t. $uv = 0$ or $vu = 0$. Since u is a unit, $\exists u^{-1} \in R$ s.t. $u^{-1}u = 1$. We have,

$$uv = 0 \implies u^{-1}uv = 0 \implies 1v = 0 \implies v = 0.$$

Similarly, $vu = 0 \implies v = 0$. Therefore, u is not a zero divisor. □

§22 Lecture 22

§22.1 Integral domains

Definition 22.1. A commutative unital ring with no zero divisors is called an *integral domain*.

Corollary 22.2

Every field is an integral domain.

Proof. Recall that a field is a commutative unital ring in which every non-zero element is a unit. Hence, by the Theorem 21.10, a field has no zero divisors and is thus an integral domain. □

Remark 22.3. The converse is not true. An example of an integral domain that is not a field is $\mathbb{Z}$.

Theorem 22.4

A finite integral domain is a field.

Proof. It suffices to show that every element of a finite integral domain has an inverse. Let R be a finite integral domain, and let $r \in R \setminus \{0\}$. Consider the set $\{r^n \mid n \in \mathbb{N}\} \subseteq R$. Since R is finite, there exists $k \in \mathbb{N}_{\geq 2}$ s.t. $r^k = r$, so $r(r^{k-1} - 1) = 0$. Since R is an integral domain, we must have $r^{k-1} - 1 = 0$ since $r \neq 0$. Equivalently, we can say that $r^{k-2}r = 1$, so r is invertible. □

Corollary 22.5

Let p be a prime number. Then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof. Since $\mathbb{Z}/p\mathbb{Z}$ is finite, it suffices to show that it is an integral domain. Let $a + p\mathbb{Z}, b + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$. Then observe that $ab + p\mathbb{Z} = 0 + p\mathbb{Z}$ if and only if $ab \in p\mathbb{Z}$, thus either $p \mid a$ or $p \mid b$, i.e. $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$, so either $a + p\mathbb{Z} = 0 + p\mathbb{Z}$ or $b + p\mathbb{Z} = 0 + p\mathbb{Z}$. Hence no zero divisor exists. Therefore $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. □

This is exactly what it means to be prime, as if ab is a multiple of p, then one of a or b must be a multiple of p. We generalise this definition below in terms of ideals.

Definition 22.6 (Prime Ideal)**.** Let R be a ring. An ideal I of R is called *prime* if I is a proper ideal, and whenever $a, b \in R$ are s.t. $ab \in I$, then one has $a \in I$ or $b \in I$.

Definition 22.7 (Maximal ideal)**.** Let R be a ring. An ideal I of R is called *maximal ideal* if I is a proper ideal and for every other ideal J s.t. $I \subseteq J \subseteq R$ we have that $J = I$ or $J = R$.

§23 Lecture 23

§23.1 Prime and maximal ideals

Definition 23.1. Let R be a ring, and $r \in R$. The set $Rr = \{xr \mid x \in R\}$ is called the *left ideal generated by* r, and this is the smallest left sided ideal containing r. The *two sided ideal generated by* r is

$$(r) = RrR = \{\text{finite sums } \sum_i x_i r y_i \mid x_i, y_i \in R\}.$$

This is the smallest two-sided ideal containing r. Moreover, if S is a subset of R, then the ideal generated by S is

$$(S) = RSR = \{\text{finite sums } \sum_{s \in S} x_s s y_s \mid x_s, y_s \in R\}.$$

Definition 23.2. Let $I \trianglelefteq R$. Then I is called a *principal ideal* if there exists an $r \in R$ such that $I = (r)$.

Example 23.3

Every ideal of $\mathbb{Z}$ is principal. This means for any ideal in $\mathbb{Z}$, there exists an integer n such that the ideal can be expressed as $(n) = \{n \cdot k \mid k \in \mathbb{Z}\}$, the set of all multiples of n.

Furthermore, an ideal (n) is a prime ideal if and only if $|n|$ is a prime number. This is because if $|n|$ is not prime, say $n = pq$ with $p,\ q \in \mathbb{Z}_{>1}$ both less than $|n|$, then pq belongs to (n) but neither p nor q would be in (n), contradicting the definition of a prime ideal.

Also, note that (n) is prime if and only if it is maximal. This is because any other proper ideal that contains (n) would have to be generated by a divisor of n, and if n is prime, its only divisors are 1 and itself.

Theorem 23.4

Let R be a ring and let I, J be ideals of R. Then $I + J = \{i + j \mid i \in I, j \in J\}$ is an ideal of R. Furthermore, it is the smallest ideal containing I and J.

Proof. Let $x, y \in I + J$, so there exists $i, i' \in I$ and $j, j' \in J$ s.t. $x = i + j$ and $y = i' + j'$. Then

$$x - y = (i + j) - (i' + j') = (i - i') + (j - j') \in I + J,$$

so $I + J$ is an additive subgroup by the subgroup test. For $r \in R$, we have that

$$r(i + j) = ri + rj \in I + J,$$

since I and J are ideals. Therefore, $I + J$ is closed under left multiplication. Similarly, $I + J$ is closed under right multiplication, hence it is an ideal.

Let L be an ideal containing I and J. Then clearly $I + J \subseteq L$ since an ideal is closed under addition, so $I + J$ must be the smallest one. □

Theorem 23.5

Let R be a commutative unital ring, and let I be a proper ideal. Then I is prime if and only if R/I is an integral domain.

Proof. Suppose that R/I is an integral domain. Let $a, b \in R$ and suppose

$$(a + I)(b + I) = 0 + I.$$

Since R/I is an integral domain, we must have that either $a \in I$ or $b \in I$, which is exactly the definition of I being prime.

Conversely, assume that I is prime and $ab \in I$ for $a, b \in R$. It follows that

$$ab + I = (a + I)(b + I) = 0 + I,$$

and since I is prime we must have either $a \in I$ or $b \in I$. Equivalently, $a + I = 0 + I$ or $b + I = 0 + I$, as required. □

Example 23.6

Let $R = \mathbb{Z}[X]$ and consider $I = (X)$. Consider the evaluation map

$$\begin{aligned} \phi : \mathbb{Z}[X] &\to \mathbb{Z} \\ f &\mapsto f(0). \end{aligned}$$

We have that $R/I \cong \mathbb{Z}$ by the FIT since ϕ has kernel I and image $\mathbb{Z}$. Since $\mathbb{Z}$ and therefore R/I is an integral domain, I is a prime ideal.

Theorem 23.7

Let R be a commutative unital ring, and let I be a proper ideal. Then I is maximal if and only if R/I is a field.

Proof. Suppose I is maximal. Let $a + I \in R/I$ and assume $a \notin I$. Consider $I + (a) \supset I$, but since I is maximal, then $I + (a) = R$. In particular, $1 \in I + (a)$, so there exists $i \in I, r \in R$ s.t. $1 = i + ra \implies ra + I = 1 + I \implies (r + I)(a + I) = 1 + I$, meaning $a + I$ is invertible. Hence, since our choice of a was arbitrary, R/I is a field.

Suppose R/I is a field and let $J \supset I$ be an ideal of R. Then there exists $x \in J$ s.t. $x \notin I$, so $x + I \neq 0 + I \in R/I$. Since R/I is a field,

$$\exists y + I \in R/I \text{ s.t. } (x + I)(y + I) = xy + I = 1 + I.$$

In other words, $\exists i \in I$ s.t. $xy + i = 1$. But $x \in J \implies xy \in J$, and $i \in I \subset J$, hence $xy + i \in J \implies 1 \in J \implies J = R$, so I is a maximal ideal. □

Corollary 23.8

Every maximal ideal in a commutative unital ring is prime.

Proof. Let R be a commutative unital ring and let I be a maximal ideal of R. Then R/I is a field, so R/I is an integral domain, hence I is prime. □

Remark 23.9. The converse is false in general. For example, consider $\mathbb{Z}[X]$ and the the prime ideal (X). We know $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ is an integral domain, but (X) is not maximal since $\mathbb{Z}$ is not a field.

Example 23.10

Let us consider an ideal that is maximal in $\mathbb{Z}[X]$. Let p be a prime number, so the ideal $(p, X) = \{pf + Xg \mid f, g \in \mathbb{Z}[X]\}$ is the polynomials where constant terms are multiples of p. The ideal is maximal as $\mathbb{Z}[X]/(p, X)$ is a field.

§24 Lecture 24

§24.1 Division with remainder of polynomials

Definition 24.1. Let F be a field, and let $f(X) = a_0 + a_1X + \cdots + a_dX^d \in F[X]$ be a polynomial with $a_d \neq 0$. Then we say the *degree* of f, written $\deg f$, is d.

Theorem 24.2 (Division with Remainder in Polynomial Rings)
Let F be a field, and let $f(X), g(X) \in F[X]$. Then there exist unique polynomials $q(X), r(X) \in F[X]$ such that

$$f(X) = g(X)q(X) + r(X),$$

where $\deg(r) < \deg(g)$ or $r(X) = 0$.

Proof. (Proof of Existence) If $\deg(g) > \deg(f)$, then take $q = 0$ and $r = f$. Now assume $\deg(g) \leq \deg(f)$. Write $f(X) = a_nX^n + \cdots + a_1X + a_0$ and $g(X) = b_mX^m + \cdots + b_1X + b_0$ with $a_n, b_m \neq 0$ and $n \geq m$. We look to prove the claim by strong induction, so we assume the theorem holds for all f_0 with $\deg(f_0) < \deg(f)$. Define

$$f_0(X) = f(X) - \frac{a_n}{b_m}X^{n-m}g(X),$$

which has $\deg(f_0) < \deg(f)$. By assumption, there exist $q_0, r \in F[X]$ with $r = 0$ or $\deg(r) < \deg(g)$ such that $f_0 = q_0g + r$. Thus,

$$f = q_0g + r + \frac{a_n}{b_m}X^{n-m}g = \left(q_0 + \frac{a_n}{b_m}X^{n-m}\right)g + r.$$

Hence f can also be expressed in the required form, so by strong induction the claim holds for all $f \in F[X]$.

(Proof of Uniqueness) Assume for contradiction that there are $q, q', r, r' \in F[X]$ such that $f = qg + r = q'g + r'$, with both r and r' either zero or with degree less than g. Then

$$g(q - q') = r' - r.$$

Since g is not the zero polynomial and $q \neq q'$, $\deg(g(q - q')) \geq \deg(g)$. This implies $\deg(r' - r) \geq \deg(g)$, contradicting the assumption that $\deg(r), \deg(r') < \deg(g)$. □

Corollary 24.3
Let F be a field and let $f \in F[X]$, $a \in F$. Then $f(a) = 0$ if and only if $\exists h \in F[X]$ s.t. $f(X) = (X - a)h(X)$.

Proof. We have $f(X) = (X - a)h(X) \implies f(a) = 0$ trivially.

Assume $f(a) = 0$. By Theorem 24.2, there exists $q(X), r(X) \in F[X]$, such that

$$f(X) = (X - a)q(X) + r(X).$$

We must have $\deg r < \deg(X - a) = 1$, so $r(X)$ is a constant. We have from our assumption that $0 = f(a) = 0 + r(a)$, hence the result follows. □

§25 Lecture 25

§25.1 Prime ideals in polynomial rings

Theorem 25.1

Let F be a field and let $f \in F[X]$ be a non-zero polynomial with $\deg f = n$. Then f has at most n roots.

Proof. Assume that f has at least $n+1$ roots in F, and k distinct roots, say $a_1, a_2, \ldots, a_k$. Let each root a_i have multiplicity m_i, so that $\sum_{i=1}^{k} m_i \geq n+1$.

Since a_1 is a root of f, by Corollary 24.3, $\exists\, g_1 \in F[X]$ s.t.

$$f(X) = (X - a_1)^{m_1} g_1(X).$$

Now, because $a_2 \neq a_1$ is also a root of f and $F[X]$ has no zero divisors, we must have $g_1(a_2) = 0$, so $\exists\, g_2 \in F[X]$ s.t.

$$g_1(X) = (X - a_2)^{m_2} g_2(X).$$

Continuing this process, we construct a (finite) sequence of non-zero polynomials $g_1, g_2, \ldots, g_k$ such that

$$f(X) = (X - a_1)^{m_1}(X - a_2)^{m_2} \cdots (X - a_k)^{m_k} g_k(X).$$

Considering the RHS, we must have $\deg f \geq \sum_{i=1}^{k} m_i \geq n+1$, contradicting that $\deg f = n$. Hence, f must have at most n roots. □

Definition 25.2. Let $f \in F[X]$ be a polynomial over a field F with $\deg f > 0$. Then f is *irreducible* over F if whenever $g, h \in F[X]$ are such that $f = gh$, one has either $\deg g = 0$ or $\deg h = 0$. If f is not irreducible, then we say it is *reducible*.

Remark 25.3. The notion of irreducibility is relative to the field you're working within; the following example demonstrates this.

Example 25.4

Consider $f(x) = X^2 + 1$. This is irreducible in $\mathbb{R}[X]$ and reducible in $\mathbb{C}[X]$, since we can write $f(x) = (X - i)(X + i)$.

The polynomial $p(x) = x^2 - 2$ is irreducible over $\mathbb{Q}[X]$ but reducible over $\mathbb{R}[X]$ as it can be factored into $p(x) = (x - \sqrt{2})(x + \sqrt{2})$, where $\pm\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

Theorem 25.5

Let F be a field and let $I \subseteq F[X]$ be an ideal. Then there exists $f \in F[X]$ such that $I = (f) = \{gf \mid g \in F[X]\}$.

Proof. If $I = \{0\}$, then $I = (0)$, so suppose I is non-trivial.

Let $f \in I$ be of minimal degree, so that $\deg f \leq \deg g$ for all $g \in I \setminus \{0\}$. We claim that $I = (f)$, that is every $i \in I$ can be expressed as fh for some $h \in F[X]$.

Certainly $(f) \subseteq I$ since I is an ideal. Let $g \in I$. Then by the Theorem 24.2, $\exists q, r \in F[X]$ s.t. $g = qf + r$, where $\deg r < \deg f$ or $r = 0$. Since I is an additive subgroup, $g - qf = r \in I$, but we assumed f was of minimal degree in I, so $r = 0$. This means that $g = qf$, so $g \in (f)$. Hence we have shown $I = (f)$. □

Remark 25.6. The previous theorem says that $F[X]$ is a *principal ideal domain*; that is, all ideals can be generated by a single element in $F[X]$. This does not hold if F is not a field (or more precisely a ring with a valid Euclidean function).

Example 25.7

Let I be the ideal of $\mathbb{Q}[X]$ generated by $(X^2 + X)$ and $(X^4 + X^3 + X)$, i.e.,

$$I = \{f(X^2 + X) + g(X^4 + X^3 + X) \mid f, g \in \mathbb{Q}[X]\}.$$

By Theorem 25.5, we know that there exists $h \in \mathbb{Q}[X]$ such that $I = (h)$. The gcd of f and g will generate the whole ideal, and in this case it is easy to see that $\gcd(f, g) = X$, so $I = (X)$.

Remark 25.8. The single generator for an ideal of $F[X]$ generated by two polynomials f and g will be their gcd. It may seem like any common factor of the two polynomials would work, and although this would be an ideal that contains the original ideal, it will contain additional elements that are not a linear combination of f and g.

As a simple example, the ideal generated by X^2 and X^3, is also just generated by X^2, but X is not a generator for the ideal since we get extra elements of degree 1 that would otherwise not be present.

§26 Lecture 26

§26.1 Irreducible polynomials

Theorem 26.1

Let F be a field, and let $f \in F[X]$ be non-zero. Then the following are equivalent

1. The ideal $(f) = \{fg \mid g \in F[X]\}$ is maximal;
2. The ideal (f) is prime;
3. The polynomial f is irreducible in $F[X]$.

Proof. $(1 \implies 2)$ Suppose (f) is maximal. Then (f) is maximal $\implies$ $F[X]/(f)$ is a field $\implies$ $F[X]/(f)$ is an integral domain $\implies$ (f) is prime. (Corollary 23.8)

$(2 \implies 3)$ Suppose the ideal (f) is prime. Consider $f = gh$ for some $g, h \in F[X]$, so $g \in (f)$ or $h \in (f)$. Assume without loss of generality that $g \in (f)$, i.e., there exists $k \in F[X]$ such that $g = fk$. Now, we have that $\deg f = \deg g + \deg h$ and $\deg g = \deg f + \deg k$. Hence, $\deg h = \deg k = 0$, so $h, k \in F$ and are units. Therefore, f is irreducible in $F[X]$.

$(3 \implies 1)$ Suppose f is irreducible in $F[X]$. For f to be irreducible, it must be of degree greater than zero and therefore (f) is a proper ideal. Assume there exists an ideal J such that $(f) \trianglelefteq J \trianglelefteq F[X]$. By Theorem 25.5, $F[X]$ is a PID, so $\exists g \in F[X]$ s.t. $J = (g)$.

Since $f \in (f) \subseteq (g)$ $\exists h \in F[X]$ s.t. $f = gh$. Since f is irreducible, either g or h is a unit. Suppose g is a unit. Then $\exists g^{-1} \in F[X]$ s.t. $gg^{-1} = 1$, so $1 \in (g) \implies J = F[X]$. Suppose now that h is a unit. Then $\exists h^{-1} \in F[X]$ with $hh^{-1} = 1$, so $f = gh \implies g = fh^{-1}$, which means $(g) \subseteq (f) \implies (g) = (f)$. We conclude (f) is maximal. □

This theorem gives us a way of easily constructing new fields.

Example 26.2

Let $F = \mathbb{Z}/3\mathbb{Z}$, which is a field. The polynomial $f(X) = X^2 + 1 \in F[X]$ is irreducible. It follows that $F[X]/(f)$ is a field. Recall that for every $g \in F[X]$ there exists $h = a_0 + a_1 x \in F[X]$ s.t. $g + (f) = h + (f)$. Hence we have

$$F[X]/f(x) = \{a_0 + a_1 X \mid a_0, a_1 \in F\}$$

Note that it has 9 elements.

Theorem 26.3

Let F be a field and let $f \in F[X]$ have degree 2 or 3. Then f is reducible if and only if it has a root in F, i.e. iff there exists $a \in F$ s.t. $f(a) = 0$.

Proof. If f is reducible, then $f = gh$ for some $0 < \deg g < \deg f$, $0 < \deg h < \deg f$ and $\deg g + \deg h = \deg f$, which implies at least one of the factors has degree 1, which is of the form $a_0 + a_1 X$ and has root $\frac{-a_0}{a_1} \in F$.

Conversely, assume $f(a) = 0$ for some $a \in F$. Then Corollary 24.3 implies $\exists h \in F[X]$ with $f = h \cdot (X - a)$. Since $X - a$ has degree 1, h must be of degree 1 or 2, depending on whether f is of degree 2 or 3 respectively, so f is reducible. □

Example 26.4

Let $d \in \mathbb{Z}$ be non-square. Then the corresponding quadratic number field is defined as

$$\mathbb{Q}[X]/(X^2 - d) \cong \mathbb{Q}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\}$$

$$a + bX + (X^2 - d) \mapsto a + b\sqrt{d},$$

where the inverse of an element $a + b\sqrt{d}$ is $\frac{a - b\sqrt{d}}{a^2 - b^2 d}$.

§27 Lecture 27

§27.1 Intermission: Classifying groups of order 21

Example 27.1

Let G be a group of order 21. How many possibilities are there for G?

Proof. We begin by noting that $21 = 7 \cdot 3$. According to Cauchy's theorem, there must exist elements in G, say $g, h \in G$, of orders 7 and 3 respectively, such that $g^7 = e = h^3$.

Define two subgroups: $K = \langle g \rangle$ and $H = \langle h \rangle$.

Observe that $K \cap H = \{1\}$, as by Lagrange's theorem, we have the size of $|K \cap H|$ divides both $|K|$ and $|H|$. Since $\gcd(|H|, |K|) = 1$, the intersection must be trivial. Furthermore, K is normal in G, as $[G : K]$ is the smallest prime divisor of $|G|$.

Consider a mapping from H to $\mathrm{Aut}(K)$ given by $h \mapsto \phi_h$. We aim to classify how many mappings we have between H and $\mathrm{Aut}(K)$ (equivalently how many options we have for ϕ_h) as this will tell us how many distinct groups we can construct via a semi-direct product of K and H. Since K is cyclic of order 7, $\mathrm{Aut}(K) \cong (\mathbb{Z}/7\mathbb{Z})^\times$, which is cyclic of order 6. One can verify there is exactly 2 mappings from $H \cong \mathbb{Z}/3\mathbb{Z}$ to $\mathrm{Aut}(K) \cong \mathbb{Z}/6\mathbb{Z}$, which define our semi-direct products. So we conclude there are 2 groups of order 21.

Now we aim to find explicitly what these 2 mappings are. Consider an automorphism ϕ_h of K defined by $\phi_h(g^i) = hg^ih^{-1}$. This map is an automorphism because it is well-defined, surjective, and its inverse is $\phi_{h^{-1}}$. We must have $hgh^{-1} = g^r$ for some $r \in \mathbb{Z}$ as K is cyclic, meaning r uniquely determines ϕ_h.

Consider $\phi_h^j(g) = h^j g h^{-j} = g^{r^j}$; our goal is to try and find a congruence equation that will allow us to solve for r and find all compatible automorphisms. Looking at $j = 3$, we require $gr^j = g$, leading to the congruence $r^3 \equiv 1 \mod 7$ which has solutions $r = 1, 2, 4$.

We know there are only 2 possible mappings, and what we have found above is the elements of $\mathrm{Aut}(K)$ which are compatible with our mapping.

First define a mapping $\varphi_1 : C_3 \to \mathrm{Aut}(C_7)$ as:

$$a \mapsto \phi_a, \text{ where } \phi_a(g) = g, \ \forall g \in C_7,$$

that is φ_1 is the trivial map. We saw in the semi-direct product section that if our mapping is trivial then the definition reduces to the familiar direct product. So we have $C_7 \times C_3 \cong C_{21}$ as 7 and 3 are coprime.

Now, define a mapping $\varphi_2 : C_3 \to \mathrm{Aut}(C_7)$ as:

$$\begin{aligned} e &\mapsto \phi_e(g) = g, \\ a &\mapsto \phi_a(g) = g^2, \\ a^2 &\mapsto \phi_{a^2}(g) = g^4, \ \forall g \in C_7 \end{aligned}$$

where $e, a \in C_3$, and $g \in C_7$. This mapping leads to the semidirect product $C_7 \rtimes_{\varphi_2} C_3$. So the only groups of order 21 are C_{21} and $C_7 \rtimes_{\varphi_2} C_3$. □

§28 Lecture 28

§28.1 Irreducibility criteria

Definition 28.1. The *content* of a nonzero polynomial $f \in \mathbb{Z}[X]$ with coefficients $a_0, a_1, \ldots, a_n$ is

$$c(f) = \gcd(a_0, \ldots, a_n).$$

Definition 28.2. A polynomial $f(X) \in \mathbb{Z}[X]$ is called *primitive* if its content is 1.

Lemma 28.3 (Gauss's Lemma - Primitivity)
The product of two primitive polynomials is also primitive.

Proof. Let $f = a_0 + a_1X + \cdots + a_nX^n$ and $g = b_0 + b_1X + \cdots + b_mX^m$ be primitive polynomials and suppose the product fg is not primitive. That is, there is a prime p that divides all coefficients of fg.

Since f and g are primitive, we can find the smallest coefficients a_r and b_s of f and g respectively that are not divisible by p. Consider the coefficient of X^{r+s} of fg:

$$\cdots a_{r-2}b_{s+2} + a_{r-1}b_{s+1} + a_rb_s + a_{r+1}b_{s-1} + a_{r+2}b_{s-2}\cdots .$$

We have that all terms containing an a_i for $i < r$ and b_j for $j < s$ are divisible by p, and a_rb_s was assumed to be not divisible by p, so overall the coefficient of X^{r+s} cannot be divisible by p, a contradiction. □

Theorem 28.4 (Gauss's Lemma - Irreducibility)
Let $f \in \mathbb{Z}[X]$ be primitive. Then f is reducible in $\mathbb{Q}[X]$ into polynomials of degree $r, s \in \mathbb{N}_{\leq n-1}$ iff it factorises as a product of degree r and s polynomials in $\mathbb{Z}[X]$.

Proof. Assume $f \in \mathbb{Z}[X]$ is primitive and can be factorised as $f(X) = g(X)h(X)$ where g and h are polynomials in $\mathbb{Z}[X]$ of degree r and s respectively. Then f is clearly reducible in $\mathbb{Q}[X]$ because $\mathbb{Z}[X] \subseteq \mathbb{Q}[X]$.

Assume now that f is reducible in $\mathbb{Q}[X]$, i.e. there exists polynomials $p(X)$ and $q(X)$ in $\mathbb{Q}[X]$ with degrees r and s respectively such that $f(X) = p(X)q(X)$. Now multiply p and q by suitable integers (lcm of denominators of coefficients), say a and b, to get new polynomials P and Q such that $P, Q \in \mathbb{Z}[X]$. We therefore have $P(X) = ap(X)$ and $Q(X) = bq(x)$ and therefore $f = \frac{1}{ab}PQ$. Factoring out the contents of P and Q gives

$$\frac{ab}{c(P)c(Q)}f = P'Q',$$

where P' and Q' are now primitive polynomials in $\mathbb{Z}[X]$. By the previous lemma, the product $P'Q'$ must remain primitive, so the coefficient of f must be ± 1, so we see that $ab = \pm c(P)c(Q)$.

Therefore, $f = \pm P'Q'$. Hence f factorises into a product of degree r and s polynomials in $\mathbb{Z}[X]$, as required. □

Example 28.5

The polynomial $X^4 + 2$ is irreducible in $\mathbb{Q}[X]$. This can be shown by contradiction.

Assume the polynomial is reducible, then $X^4 + 2 = fg$ for some $f, g \in \mathbb{Q}[x]$. We have two cases; we must have either (WLOG) $\deg f = 1$ and $\deg g = 3$, or both $\deg f = \deg g = 2$.

For the first case, f and therefore $X^4 + 2$ has a root in $\mathbb{Q}$. But we have that $X^4 + 2$ is strictly positive, and therefore does not cross the origin, so this is not possible.

Now consider the second case. By Gauss's Lemma, it suffices to show that $X^4 + 2$ has no factorization in $\mathbb{Z}[X]$. Assume $f, g \in \mathbb{Z}[X]$, s.t. $f = a_2x^2 + a_1x + a_0$, $g = b_2x^2 + b_1x + b_0$. Note that since X^4 has coefficient 1, we must have $a_2 = b_2 = 1$ (similar when $a_2 = b_2 = -1$). Expanding the product fg gives

$$fg = a_2b_2X^4 + (a_2b_1 + a_1b_2)X^3 + (a_2b_0 + a_1b_1 + a_0b_2)X^2 + (a_1b_0 + a_0b_1)X + a_0b_0.$$

We can see that we must have $a_0b_0 = 2$. Let $a_0 = 1$ and $b_0 = 2$. We must have $a_2b_0 + a_0b_2 + a_1b_1 = 0$ for the X^2 term to cancel out. Equivalently, we must have $a_1b_1 = -3$. There are two choices for a_1 and b_1; consider $a_1 = -1$ and $b_1 = 3$. We must have $a_1b_0 + a_0b_1 = 0$ for the X term to cancel out, but we have $-1 + 6 = 5 \neq 0$; a contradiction.

Note that the argument is the same for any choice of coefficients of f and g we could have made; for example, taking $a_0 = -1$ and $b_0 = -2$ or $a_1 = 1$ and $b_1 = -3$.

Theorem 28.6 (Eisenstein's Criterion)

Let p be a prime number, and let $f(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ be s.t. $p \nmid a_n$, $p \mid a_i$ for all $i < n$, and $p^2 \nmid a_0$. Then f is irreducible in $\mathbb{Q}[X]$.

Proof. Let $f(x)$ be as in the statement. The aim is to show that $f(x)$ does not factor into a product of two polynomials in $\mathbb{Z}[X]$. We will assume for contradiction that $f(x) = g(x)h(x)$, where $g(x) = b_rx^r + \cdots + b_0 \in \mathbb{Z}[X]$ and $h(x) = c_sx^s + \cdots + c_0 \in \mathbb{Z}[X]$, and $r + s = n$. We have,

$$a_nx^n + \ldots + a_0 = b_rc_sx^{r+s} + \cdots + b_0c_0.$$

We must have $a_n = b_rc_s$ and $a_0 = b_0c_0$. Since a_n, and therefore both b_r and c_s, is not divisible by p, we must have that all the b_i and c_i $(i < n)$ are divisible by p or there would exist a term in $g(x)h(x)$ with degree less than n with a coefficient that is not divisible by p after distributing. In particular, p must divide both b_0 and c_0, which means that p^2 divides $b_0c_0 = a_0$, a contradiction. Therefore, no such $g(x)$ and $h(x)$ exist, so f is irreducible in $\mathbb{Q}[X]$. □

Example 28.7

Let p be a prime number. We have that $f(X) = X^{p-1} + \cdots + X + 1$ is irreducible in $\mathbb{Q}[X]$. To show this, note that $f(X) = g(X)h(X)$ iff $f(X+1) = g(X+1) = h(X+1)$ (invertible substitution), so it suffices to show that $f(X+1)$ is irreducible.

Explicitly computing $f(X+1)$ for different primes p, we see that the coefficients are all but the last term in the p^{th} row of Pascal's triangle. For example, for $p = 5$,

$$f(X+1) = X^4 + 5X^3 + 10X^2 + 10X + 5.$$

We can see that such a polynomial satisfies Eisenstein's Criterion, and is therefore irreducible.

The following example is a slight aside on what was done in this lecture, however it is important to see.

Example 28.8

Consider the group $A = (\mathbb{Z} \times \mathbb{Z}, +)$. The set of homomorphisms from A to A forms a ring under

$$(f+g)(a) = f(a) + g(a)$$
$$(fg)(a) = f(g(a)) \ \forall a \in A$$

For all $f, g : A \to A$. A homomorphism from a group to itself is called an endomorphism. The set of endomorphisms with these two operations is called the endomorphism ring, called $\text{End}(A)$. We claim this ring is noncommutative. Take as an example $\phi : (m,n) \mapsto (0,n)$ (a ring homomorphism), and $\psi : (m,n) \mapsto (m+n, 0)$. Then note $\phi\psi : (m,n) \mapsto (0,0)$, and $\psi\phi : (m,n) \mapsto (n,0)$, hence they are not the same: take $(\phi\psi)(0,1) = (0,0) \neq (\psi\phi)(0,1) = (1,0)$. In fact, note that these two elements serve as a basis for the whole ring – we can get any (m,n) by $m(1,0)+n(0,1)$.

Note that earlier in the course we talked about Automorphisms, which are really just invertible endomorphisms. And following the above example, it follows that $\text{Aut}(A) = (\text{End}(A))^\times$, the group of units of $\text{End}(A)$.

§29 Lecture 29 - (Non-Examinable from now on)

§29.1 An Aside on Free groups

Free groups are an essential concept in group theory, providing a fundamental example of how groups can be constructed. The idea is to start with a set S and create a group that has the least possible number of relations among elements of S needed to form a group.

A free group can be thought of as a group formed by all possible "words" created from elements of S and their inverses, subject only to the most basic requirements of a group. The crucial point is that no additional relations (like commutativity or specific element properties) are imposed beyond those necessary for a group structure.

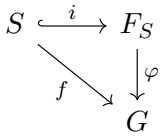
Definition 29.1 (Free Group - Constructive Approach)**.** Let S be a set. Form the set T where each element is the inverse of a unique element of S, and vice versa. Consider the set of all "words" formed by concatenating elements from $S \cup T$, including an empty

word e as the identity.

The *free group* on S, denoted F_S, consists of all such words reduced to their simplest form via the elimination of adjacent inverse pairs. The group operation is concatenation followed by this reduction, ensuring the group axioms are satisfied.

Remark 29.2. The constructive definition provided above is intentionally broad and conceptual, aimed at offering an intuitive understanding of free groups. For our purposes, we will primarily utilize the definition based on the universal property, as it proves two key general theorems more efficiently. One can find a rigorous construction of free groups online.

Definition 29.3 (Free Group - Universal Property)**.** The free group F_S on a set S is characterized by the following universal property: for any function f from S to a group G, there exists a unique group homomorphism φ from F_S to G making the following diagram commute:



Here, i is the inclusion map of S into F_S.

Theorem 29.4

Every group G is the quotient of a free group F_X by some normal subgroup N.

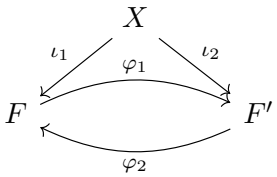
Proof. We know that by the universal property of free groups, f extends to a unique φ, where $\varphi : F_X \to G$ is a group homomorphism. Take $f : X \to G$ to be the canonical inclusion map, where X is the underlying set of G, and define $\varphi(x) = f(x)$. Then φ is clearly surjective onto G. By the FIT, $F_X/\ker\varphi \cong G$. So, $N = \ker\phi$ satisfies the statement of the theorem. □

Theorem 29.5 (Uniqueness of Free Groups)

Let F and F' be free groups on the set X. Then $F \cong F'$

Proof. Suppose F and F' are both free groups on the set X. We want to show that F and F' are isomorphic.

By the universal property of F, for any function $\iota_2 : X \to F'$, there exists a unique group homomorphism $\varphi_1 : F \to F'$ such that $\varphi_1 \circ \iota_1 = \iota_2$, where $\iota_1 : X \to F$ is the inclusion map. Similarly, for the universal property of F' we get $\varphi_2 \circ \iota_2 = \iota_1$. This gives the following diagram.



Substituting gives $\iota_1 = (\varphi_2 \circ \varphi_1) \circ \iota_1$ and $\iota_2 = (\varphi_1 \circ \varphi_2) \circ \iota_2$. So by the uniqueness of the universal property, $\varphi_2 \circ \varphi_1 = \mathrm{id}_F$ and $\varphi_1 \circ \varphi_2 = \mathrm{id}_{F'}$, so ϕ_1 is an isomorphism and $F \cong F'$ as required. □

§30 Lecture 30

§30.1 Field Extensions

Definition 30.1 (Field Extension)**.** Suppose K is a field, and let F be a field containing K. Then F/K is a *field extension*.

Remark 30.2. With groups and rings, typically we find it useful to look inward to substructures (subgroups and ideals), however the interest with fields is to look outward to extensions. This is because if F/K is a field extension, we can view F as a vector space over K. The notation F/K does not imply a quotient like it might in other algebraic structures. Instead, it is simply a way to describe the field F as a structure that contains K and has a vector space structure relative to K.

Example 30.3

The following is a familar example of a field extension: $\mathbb{C}/\mathbb{R}$ – a 2-dim vector space over $\mathbb{R}$ (the *complex plane*).

This is a more interesting example to think about: $\mathbb{R}/\mathbb{Q}$ – an ∞-dim (uncountably) vector space over $\mathbb{Q}$.

Example 30.4

A more useful definition of a field extension comes from considering embeddings into bigger fields and not just actual set containment.

Let K be a field and consider an irreducible polynomial $f \in K[X]$. Then we can define $F = K[X]/(f)$; this is a field.

Note that K is not contained in F in the regular notion of set containment, but it can be embedded into F.

Consider the quotient map $\phi : K[X] \to K[X]/(f)$, $g \mapsto g + (f)$. Observe that K is actually a subring of $K[X]$ (constant polynomials).

Consider the map ϕ restricted to K, $\phi|_K$. An irreducible polynomial has degree at least 2, therefore, for $\phi(k) = k + (f) = 0$, k must have degree at least 2. So, $\phi|_K$ is injective as it consists only of degree 0 polynomials (and zero).

We can conclude that F/K is a field extension.

Remark 30.5. Notice that in the example above, we do not have that the set K is actually contained in F, but rather that it can be naturally embedded into F. Because of this, we can still view F/K as a field extension.

Example 30.6

Consider $K = \mathbb{R}$ and $f = X^2 + 1 \in \mathbb{R}[X]$, which is irreducible. Define $F = \mathbb{R}[X]/(f)$ which is a 2-dimensional field extension of $\mathbb{R}$ with basis $1 + (X^2 + 1), X + (X^2 + 1)$. Let α be the image of X under the previous quotient map

$$\begin{aligned} \phi : K[X] &\to K[X]/(X^2 + 1) \\ k &\mapsto k + (X^2 + 1). \end{aligned}$$

Notice $\alpha^2 + 1 = 0 + (X^2 + 1)$ in F, so α satisfies $g(t) = t^2 + 1 \in K[X]$. Thus F is isomorphic to $\mathbb{C}$.

Theorem 30.7

Let K be a field and let $f \in K[X]$ with $\deg f > 0$. Then there exists a field extension F/K and $\alpha \in F$ s.t. $f(\alpha) = 0$.

Proof. Let $f = gh$ where g is irreducible. Define $F = K[X]/(g)$. Then take $\alpha = X + (g)$, and so $g(\alpha) = g(X) + (g) = 0 + (g)$, so $f(\alpha) = g(\alpha)h(\alpha) = 0$. □

Definition 30.8. Let F/K be a field extension, and $\alpha \in F$. We say α is *algebraic* over K if there exists $f \in K[X] \setminus \{0\}$ s.t. $f(\alpha) = 0$. If there is no such polynomial, we say that α is *transcendental* over K.

Example 30.9

For all $d \in \mathbb{Q}$, $\sqrt{d} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, consider $f(x) = x^2 - d \in \mathbb{Q}[X]$.

For all $n \in \mathbb{Z}_{>0}$, $e^{2\pi i/n} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, consider $f(x) = x^n - 1$.

Transcendental elements of $\mathbb{C}$ include e and π, but proving they are transcendental is very difficult.

Theorem 30.10

Let F/K be a field extension, and let $\alpha \in F$ be algebraic over K. Then there exists an irreducible polynomial $p \in K[X]$ with $p(\alpha) = 0$, and for all $f \in K[X]$ with $f(\alpha) = 0$, we have p divides f in $K[X]$.

Proof. First, α being algebraic over K implies that there exists $f \in K[X] \setminus \{0\}$ with $f(\alpha) = 0$. Let $p \in K[X]$ be such an f with the smallest degree, so $p(\alpha) = 0$. Assume for contradiction that p is reducible, i.e., there exists $g, h \in [X]$ with degrees $r, s < n$ respectively, such that $f = gh$. This means that $f(\alpha) = g(\alpha)h(\alpha) = 0$, so we must have $g(\alpha) = 0$ or $h(\alpha) = 0$. This is a contradiction as we have assumed that p is the smallest such polynomial, therefore p must be irreducible over $K[X]$.

Now suppose that $f \in K[X]$ with $f(\alpha) = 0$, by the division algorithm we can write $f = pq + r$ where $\deg r < \deg p$. We have 2 cases, if $r = 0$ then $f = pq$ so p divides f. Assume $r \neq 0$ then we have that $r(\alpha) = f(\alpha) - p(\alpha)q(\alpha) = 0$, but as p was minimal degree, it follows that $r = 0$, and so $f = pq$ as required. □

Corollary 30.11

Let F/K be a field extension, and let $\alpha \in F$ be algebraic over K. Let $p, p' \in K[X]$ be irreducible polynomials s.t. $p(\alpha) = p'(\alpha) = 0$. Then $\exists \lambda \in K$ s.t. $p = \lambda p'$.

Proof. We have from theorem 30.10 that $p \mid p'$ and $p' \mid p$. This implies $\deg p = \deg p'$, and the result follows. □

Definition 30.12. A polynomial $f = a_n x^n + \cdots + a_0 \in K[X]$ is called *monic* if $a_n = 1$. Let F/K be an extension field and α be algebraic over K. The unique monic irreducible polynomial $p \in K[X]$ s.t. $p(\alpha) = 0$ is called the irreducible polynomial of α over K, or the minimal polynomial of α over K, written as $\operatorname{irr}(\alpha, K)$.

Example 30.13

Recall that if $n \in \mathbb{Z}$, then $e^{2\pi i/n} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^n - 1$.

Let $\alpha = e^{2\pi i/n}$ and suppose that n is prime. Then $\operatorname{irr}(\alpha, K) = X^{n-1} + X^{n-2} + \cdots + 1$. This polynmial is known to be irreducible over the rationals when n is prime, and it has root α. We can show this by Eisenstein's criterion after using translation by 1, as in Example 28.7.

§31 Lecture 31

§31.1 Field Extensions and Degrees

Definition 31.1. Let F/K be a field extension and $\alpha \in F$ be algebraic over K. The *degree of α over K*, written $\deg(\alpha, K)$, is the degree of the polynomial $\operatorname{irr}(\alpha, K)$. The *degree of F over K* , written $[F : K]$ is the dimension of F as a vector space over K. An extension F/K is finite if $[F : K] < \infty$.

Definition 31.2. Let $K(\alpha)$ denote the smallest subfield of F that contain K and α, the field generated by α over K.

It can be shown that $K(\alpha)$ is exactly the range of the evaluation map at α for polynomials over K. More precisely, $K(\alpha) = \{f(\alpha) \mid f \in K[X]\}$. We use this fact to prove the following theorem.

Theorem 31.3

Let F/K be a field extension, $\alpha \in F$ be algebraic over K. Then $[K(\alpha) : K] = \deg(\alpha, K)$. More precisely, every element of $K(\alpha)$ can be uniquely written as $b_0 + b_1\alpha + \cdots b_{d-1}\alpha^{d-1}$ where $d = \deg(\alpha, K)$ and $b_i \in K$. In other words, $1, \alpha, \ldots, \alpha^{d-1}$ is a basis for $K(\alpha)$ over K as a vector space.

Proof. Let $f \in K$. Since $K(\alpha)$ is the range of the evaluation map, $f(\alpha)$ is an arbitrary element of $K(\alpha)$. By the division algorithm, $\exists!\, q, r \in K$ s.t. $f = q \cdot \operatorname{irr}(\alpha, K) + r$, where $\deg(r) < \deg(\alpha, K) = d$, or $r = 0$.

Evaluating at α, we have that $f(\alpha) = 0 + r(\alpha)$, i.e. $\exists\, b_i \in K$ s.t. $f(\alpha) = b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1}$. Hence $f(\alpha)$ can be expressed as a linear combination of $1, \alpha, \ldots, \alpha^{d-1}$, so the set spans $K(\alpha)$.

Suppose $b_0 + b_1\alpha + \ldots + b_{d-1}\alpha^{d-1} = 0$, where not all b_i are zero. This is saying that α is a root of a polynomial of degree at most $d-1 < d$, which contradicts the assumption that $d = \deg(\alpha, K)$, so the set is linearly independent.

Suppose two distinct linear combinations were equal, i.e. $\exists b_i, b_i' \in K$ s.t.

$$b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1} = b_0' + b_1'\alpha \cdots + b_{d-1}'\alpha^{d-1}.$$

This would mean that

$$(b_0 - b_0') + (b_1 - b_1')\alpha + \cdots + (b_{d-1} - b_{d-1}')\alpha^{d-1} = 0,$$

so $b_0 = b_0'$, $b_1 = b_1'$, …, $b_{d-1} = b_{d-1}'$, since we have linear independence. □

§32 Lecture 32

§32.1 Algebraic Closure

Theorem 32.1

Let L/F and F/K be field extensions. Then L/K is finite if and only if L/F and F/K are both finite. Moreover, if this is the case, we have $[L:K] = [L:F][F:K]$. More precisely, if $\alpha_1, \cdots, \alpha_n$ is an F-basis for L, and $\beta_1, \cdots, \beta_m$ is a K-basis for F, then $\{\alpha_i\beta_j : 1 \le i \le n, 1 \le j \le m\}$ is a K-basis for L.

Proof. We will show that $\{\alpha_i\beta_j : 1 \le i \le n, 1 \le j \le m\}$ is linearly independent and spans L. Let $l \in L$. Since $\alpha_1, \cdots, \alpha_n$ is an F-basis for L, we can write $l = f_1\alpha_1 + f_2\alpha_2 + \cdots + f_n\alpha_n$, where $f_i \in F$. Now, since $\beta_1, \cdots, \beta_m$ is a K-basis for F, we have that each $f_i = k_{i1}\beta_1 + k_{i2}\beta_2 + \cdots + k_{im}\beta_m$, where $k_{ij} \in K$. Therefore,

$$\begin{aligned} l &= (k_{11}\beta_1 + \cdots + k_{1m}\beta_m)\alpha_1 + \cdots + (k_{n1}\beta_1 + \cdots +_{nm} \beta_m)\alpha_n \\ &= (k_{11}\alpha_1\beta_1 + \cdots + k_{1m}\alpha_1\beta_m) + \cdots + (k_{n1}\alpha_n\beta_1 + \cdots +_{nm} \alpha_n\beta_m). \end{aligned}$$

We have therefore shown that an arbitrary element $l \in L$ can be expressed as a K-linear combination of $\alpha_i\beta_j$, therefore $\{\alpha_i\beta_j : 1 \le i \le n, 1 \le j \le m\}$ spans L.

To show linear independence, assume we have constants $c_{11}, \cdots, c_{nm}$ in K such that

$$c_{11}\alpha_1\beta_1 + c_{12}\alpha_1\beta_2 + \cdots + c_{nm}\alpha_n\beta_m = 0.$$

Factor out the α_i's,

$$\alpha_1(c_{11}\beta_1 + c_{12}\beta_2 + \cdots + \cdots + c_{1m}\beta_m) + \cdots + \alpha_n(c_{n1}\beta_1 + \cdots + c_{nm}\beta_m) = 0.$$

We have that

$$\begin{aligned} c_{11}\beta_1 + c_{12}\beta_2 + \ldots + c_{1m}\beta_m &= 0 \\ c_{21}\beta_1 + c_{22}\beta_2 + \ldots + c_{2m}\beta_m &= 0 \\ &\vdots \\ c_{n1}\beta_1 + c_{n2}\beta_2 + \ldots + c_{nm}\beta_m &= 0, \end{aligned}$$

and since the β_i's form a basis, they are linearly independent, so we can conclude that all the c_{ij}'s are 0, and therefore $\{\alpha_i\beta_j\}$ are linearly independent. □

Definition 32.2. We denote

$$\overline{K_F} := \{\alpha \in F \mid \alpha \text{ is algebraic over } K\}$$

and read it as the *algebraic closure* of K in F.

Lemma 32.3

Let F/K be a field extension and let V be a finite dimensional non-trivial K-vector space. If $\alpha \in F$ and $\alpha V \subset V$, then $\alpha \in \overline{K_F}$.

Proof. Let $\{v_1, v_2, \ldots, v_n\}$ be a K-basis for V. We have $\alpha V \subset V \implies \alpha v_i = k_{i1}v_1 + k_{i2}v_2 + \cdots + k_{in}v_n$, where $k_{ij} \in K$. We can then construct a matrix representation for α, call it A. The matrix is as follows:

$$A = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ k_{n1} & \cdots & \cdots & k_{nn} \end{bmatrix}.$$

This matrix has been constructed in a way such that $A(v) = \alpha v$ for $v \in V$ (as $A(v_i) = k_{i1}v_1 + k_{i2}v_2 + \cdots + k_{in}v_n = \alpha v_i$). So we have that the characteristic polynomial $\chi(X) = \det(\alpha\mathbb{I}_n - A) \in K[X]$, and as α is an eigenvalue for A, it satisfies $\chi(X)$, and so α is algebraic over K, or equivalently, $\alpha \in \overline{K_F}$. □

Theorem 32.4

Let F/K be a field extension. Then $\overline{K_F}$ is a field.

Proof. Take any $\alpha, \beta \in \overline{K_F}$. Consider the K-vector space V spanned by the set $S = \{\alpha^i\beta^j \mid i, j \geq 0\}$. V is finite-dimensional because α and β satisfy some algebraic relations over K.

We aim to show that $(\alpha - \beta)V \subseteq V$ and $(\alpha\beta^{-1})V \subseteq V$. For any $v \in V$, written as a linear combination of elements in S, the expression $(\alpha - \beta)v$ results in terms of the form $\alpha^{i+1}\beta^j - \alpha^i\beta^{j+1}$, which belong to V. Hence, $(\alpha - \beta)V \subseteq V$.

Similarly, $(\alpha\beta^{-1})v$ will yield terms like $\alpha^{i+1}\beta^{j-1}$, also within V. Therefore, by lemma 32.3, $\alpha - \beta$ and $\alpha\beta^{-1}$ are in $\overline{K_F}$, confirming that $\overline{K_F}$ is indeed a field. □

Definition 32.5. A field F is called *algebraically closed* if every $f \in F[X]$ with $\deg f > 0$ has a root in F.

Theorem 32.6 (Fundamental Theorem of Algebra)

The field $\mathbb{C}$ is algebraically closed.

Sketch Proof. We go by way of contradiction. Assume there exists a field F with $\mathbb{C} \subset F$ that is a proper normal extension of $\mathbb{R}$. That is every polynomial with coefficients in $\mathbb{R}$ splits into linear factors over F. If such an F exists, then $\mathbb{C}$ would not be algebraically closed, since there would exist $\alpha \in F \setminus \mathbb{C}$ a root of a polynomial over $\mathbb{R} \subset \mathbb{C}$.

We focus on the Galois group $G = \mathrm{Gal}(F/\mathbb{R})$, which is the group of automorphisms of F that fix $\mathbb{R}$. Let $|G| = 2^n t$ where $n, t \in \mathbb{Z}_{\geq 0}$ and t is odd. Using the first Sylow Theorem there exists a Sylow-2-Subgroup, call it H with $|H| = 2^n$, and if $n = 0$, let H be the trivial group. Let F^H be the field of all elements in F fixed by every automorphism in H. That is $F^H = \{x \in F \mid \forall h \in H, h(x) = x\}$. From the Fundamental Theorem of Galois theory we know that the degrees of the extensions are related to the order of the associated Galois groups. So we have

$$|H| = \deg(F/F^H) = [F : F^H] = 2^n$$

and from Theorem 32.1 we have

$$\deg(F/\mathbb{R}) = \deg(F/F^H)\deg(F^H/\mathbb{R}) = [F : F^H][F^H : \mathbb{R}] = 2^n t,$$

which implies $\deg(F^H/\mathbb{R}) = [F^H : \mathbb{R}] = t$.

By the Primitive Element Theorem, which states that every finite separable extension can be generated by a single element, we have $F^H = \mathbb{R}(\beta)$ for some $\beta \in F$. This implies that $\deg(\beta, \mathbb{R})$ is odd and has no root in $\mathbb{R}$ as $\mathrm{irr}(\beta, \mathbb{R})$ is irreducible. However, every odd polynomial over $\mathbb{R}$ has a root in $\mathbb{R}$ as a consequence of the Intermediate Value Theorem, so we reach a contradiction. Hence, there cannot exist a proper normal extension $F/\mathbb{R}$ which implies that $\mathbb{C}$ is algebraically closed, as required. □

Remark 32.7 (Jordan Baillie Waffle)**.** Would you consider the completion of a field analytic or algebraic? Most would say analytic, however this is if you view it in the conventional sense (Cauchy Sequences, Dedekind Cuts, etc). One can view the completion of a field as a closed set (with respect to profinite topology under inverse limit) of the underlying Galois group, which is definitely in the algebraic corner. With this, you can argue that there are proofs of the Fundamental Theorem of Algebra using only algebraic methods.

Corollary 32.8

Every polynomial $f \in \mathbb{C}[X]$ of degree n has exactly n roots in $\mathbb{C}$, when counting individually any repeated roots.

Proof. By Theorem 32.6, if f is a complex polynomial of degree n, then f has a root α_1, i.e. we can write f as $(x - \alpha_1)f_1(x)$, where $\deg(f_1) = n - 1$. Again, f_1 must have a root α_2, so $f = (x - \alpha_1)(x - \alpha_2)f_2(x)$, where $\deg(f_2) = n - 2$. Repeating this process inductively, we are able to factorise f completely as $(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$. In other words, a polynomial of degree n over $\mathbb{C}$ has exactly n roots in $\mathbb{C}$. □

Theorem 32.9 (Existence of Algebraic Closure)

Every field K has an algebraic extension that is algebraically closed.

Proof. Exercise. □